Symantec™ Server Management Suite 7.5 SP1 powered by Altiris™ technology Release Notes

Symantec

Symantec™ Server Management Suite 7.5 SP1 powered by Altiris™ technology Release Notes

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Altiris, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Technical Support 4

Chapter 1 Server Management Suite 7.5 SP1 10

About Server Management Suite 10
What has changed in the release notes 11
Components of Server Management Suite 7.5 SP1 12
What's new in this release 13
What's new in Symantec Management Platform 13
What's new in ITMS Management Views 16
What's new in Server Management Suite 18
System requirements and supported platforms 21
General installation and upgrade information 21
Other things to know 26
Where to get more information 27

Chapter 2 Deployment Solution 30

What's new in Deployment Solution 30
Known Issues 31
Fixed Issues 42

Chapter 3 Inventory Solution 43

Known issues 43
Fixed issues 61
Other things to know 62

Chapter 4 Inventory for Network Devices 65

Known issues 65
Fixed issues 65
Other things to know 66

Chapter 5 Monitor Solution for Servers 68

What's new in this release 68
Known issues 68

Other things to know 74

Chapter 6 Patch Management Solution for Linux 77

Known issues 77
Fixed issues 80
Other things to know 81

Chapter 7 Patch Management Solution for Mac 84

Known issues 84
Fixed issues 85
Other things to know 85

Chapter 8 Patch Management Solution for Windows 87

Known issues 87
Fixed issues 94
Other things to know 95
New virtual directory behavior 97

Chapter 9 Real-Time System Management 101

Known issues 101

Chapter 10 Software Management Solution 108

What's new in this release 108
Known issues 109
Fixed issues 116
Other things to know 118

Chapter 11 Symantec Endpoint Protection Integration Component 121

About Endpoint Protection Integration Component 121
Known issues 121

Chapter 12 Virtual Machine Management 125

What's new in this release 125
System requirements 127
Installing 127
Supported hypervisors 128
Known issues 128
Fixed issues 130

Other things to know 131

Chapter 13 Workflow Solution 133

What's new in Workflow Solution 133
Known issues 136
Fixed issues 137

Chapter 1

Server Management Suite 7.5 SP1

This chapter includes the following topics:

- About Server Management Suite
- What has changed in the release notes
- Components of Server Management Suite 7.5 SP1
- What's new in this release
- System requirements and supported platforms
- General installation and upgrade information
- Other things to know
- Where to get more information

About Server Management Suite

Server Management Suite combines the essential tools that help you effectively manage your physical servers and virtual servers, reduce service interruptions, and increase uptime.

Server Management Suite incorporates a variety of wizards and other features that let you automate configuration, stage tasks, and create policies to manage your servers. Various graphical reports let you quickly identify the health of your environment, pinpoint problems, and analyze trends. Expanded support for virtual technologies simplifies the management of multiple operating system environments.

Server Management Suite is a collection of solutions that run on the Symantec Management Platform that provides the following key features:

- Discovery and inventory
  The suite automatically identifies the devices that are found in your network, and aggregates inventory data across your environment. Multi-platform support makes it easy to consolidate the discovery data of all your Windows, UNIX, and Linux assets within an integrated console. You can easily assess security vulnerabilities, prepare for software audits, and more accurately determine hardware availability and needs.
- Provisioning
  The suite lets you improve the consistency and increase the quality of server configurations. It delivers the comprehensive deployment capabilities that include image-based or scripted operating system installation and continuous provisioning. The suite helps you implement the standardized configurations, and provides you the tools for migration.
- Software distribution and patch management
  The suite lets you control server configurations through its software management capabilities. The automated policies for software and patch management help you keep the servers standardized and secure. You can modify similar configurations on multiple servers simultaneously. You can distribute applications, and security updates to target systems.
- Proactive monitoring and alerting
  The suite helps you proactively monitor the critical components of your network. You can increase the network uptime with the self-healing remediation tasks that are configured before the critical events occur. You can organize your servers into vital groups and quickly ascertain the current health of the whole network. The monitoring capabilities provide you also a summarized view of each single server performance over time.

See "Where to get more information" on page 27.

What has changed in the release notes

In the IT Management Suite 7.5 SP1 release, to make the release information easier to find and access, the release notes information of most solutions are now part of the following release notes:

- IT Management Suite 7.5 SP1
- Asset Management Suite 7.5 SP1
- Client Management Suite 7.5 SP1
- Symantec Management Platform 7.5 SP1

For more information about the changes in the release notes see the following link:

http://www.symantec.com/docs/DOC7354

Components of Server Management Suite 7.5 SP1

Server Management Suite is a collection of solutions that run on the Symantec Management Platform. These solutions let you discover, inventory, monitor, and provision servers from a central console - the Symantec Management Console.

See "About Server Management Suite" on page 10.

Table 1-1 Components of Server Management Suite

Component	Link to User Guide
Symantec Management Platform	DOC7220
Deployment Solution	DOC7207
Inventory Solution	DOC7217
Inventory for Network Devices	DOC7311
Monitor Solution for Servers	DOC7212
Monitor Pack for Servers	DOC7212
Patch Management Solution	■ Patch Management Solution for Linux: DOC7382 ■ Patch Management Solution for Mac: DOC7216 ■ Patch Management Solution for Windows: DOC7333
Real-Time System Manager	DOC7211
Software Management Solution	DOC7341
Symantec Endpoint Protection Integration Component	DOC5671
Virtual Machine Management	DOC7229
Symantec Workflow Solution	DOC7224
Topology viewer	DOC7225
Server Resource Manager view	DOC7225
Linux and UNIX Management Guide with Symantec™ Server Management Suite 7.5 SP1 powered by Altiris™ technology	DOC7219

Table 1-1 Components of Server Management Suite *(continued)*

Component	Link to User Guide
Altiris Client Management Suite 7.5 SP1 from Symantec User Guide for Mac Management	DOC7336

What's new in this release

In Server Management Suite 7.5 SP1, new features can be categorized into general enhancements in Symantec Management Platform, enhancements in ITMS Management Views (previously known as Enhanced Console Views), and enhancements in the Server Management Suite solutions.

General enhancements and new features of Symantec Management Platform and the solutions of Server Management Suite 7.5 SP1 are as follows:

- Symantec Management Platform 7.5 SP1
  See "What's new in Symantec Management Platform" on page 13.
- ITMS Management Views (previously known as Enhanced Console Views)
  See "What's new in ITMS Management Views" on page 16.
- Server Management Suite 7.5 SP1
  See "What's new in Server Management Suite" on page 18.

What's new in Symantec Management Platform

In the Symantec Management Platform 7.5 SP1, the following new features are introduced:

Table 1-2 List of new features

Feature	Description
The list of supported operating systems has been expanded.	The following operating system is now supported for installation of Symantec Management Platform and its components: ■ Windows Server 2012 R2 The following operating systems are now supported for installation of package and task servers: ■ Windows 8 ■ Windows 8.1 ■ Windows Server 2012 ■ Windows Server 2012 R2

Table 1-2 List of new features *(continued)*

Feature	Description
The list of supported client operating systems has been expanded.	The following operating systems are now fully supported for the installation of Symantec Management Agent: ■ Windows Server 2012 R2 ■ Windows 8.1 ■ OS X 10.9 ■ Windows Embedded Standard 7 SP1 ■ Red Hat Enterprise Linux 5.10 ■ VMware ESXi 5.5 **Note:** Deployment Solution supports only **Install Linux/ESX OS** task. You cannot install the Deployment Solution Plug-in and the ULM agent on the same. For support statements and other information on supported operating systems, see the following article: http://www.symantec.com/connect/articles/it-management-suite-os-platform-support
Various Notification Server performance improvements.	The following elements of Symantec Management Console were improved to provide better user experience: ■ Handling of right-click actions. ■ Improved creation of new filters. ■ Improved responsiveness of **Reports** list. ■ Shared schedules page now contains information on number of items that use a given schedule. ■ **Edit filter** window now lets you list resources from a specific Organizational Group. ■ **Edit Item Link** dialog box is now reworked to improve performance. ■ When you edit a filter, and try to save it, but in the meantime the same filter is modified by someone else, a warning message is displayed. ■ In the **Filtering Rules** window, the handling of read-only targets and scrolling is now improved. Additionally, the following items were improved: ■ Implementation of schedules is reworked to improve performance. ■ Offline agent installation package is now smaller and takes significantly less time to create. ■ Detection of client operating systems is now improved. ■ Virtual Data Class now supports DATE and DATETIME SQL data types. **Note:** DATETIMEOFFSET and TIME types are not supported.

Table 1-2 List of new features *(continued)*

Feature	Description
Hierarchy and replication improvements	The following elements of hierarchy and replication functionalities are now improved: ■ Hierarchy performance and scalability. ■ **Hierarchy and Replication** settings are now placed in single folder in Symantec Management Console. ■ **Jobs Management** page is introduced to review and manage hierarchy and replication jobs. This page also lets you troubleshoot hierarchy and replication issues in an efficient way. ■ **Replicate Now** security privilege is introduced. It allows running replication of a given item from the context menu.
Expanded reporting and error handling	The following new reports have been introduced: ■ Internet gateway status reporting. ■ **Legacy Agent Registration Requests** reporting. ■ **Package Status By Package Server** report. Error messages that are logged in Notification Server or client computer logs are reworked. Error messages are more informative.
Expanded capabilities of Data Connector and Active Directory Import.	Data Connector now contains a new resource lookup key to import subnets. The following Active Directory Import improvements have been introduced: ■ Import of multiline attributes is now supported. ■ For existing resources, you can now choose to overwrite data in CMDB or to import only new data classes. ■ You can now choose to import data only if the source item is **Managed** or **Unmanaged**. You can also import all resources, regardless of their state. ■ **Microsoft Active Directory Import** webpage now contains information on last run time.
Support for Internet Explorer 10 and Internet Explorer 11 in Symantec Management Console.	You can now use Internet Explorer 10 and Internet Explorer 11 in Compatibility mode to access Symantec Management Console.

Table 1-2 List of new features *(continued)*

Feature	Description
Installation of SSL certificates is simplified.	You can now use the **Targeted Agent Settings** webpage, to install SSL certificates on client computers. You can now import new certificates in a `.pfx` file format, that lets you reassign client computers to a different Notification Server when using HTTPS. The **Cloud-enabled Management Site Server Settings** policy lets you distribute SSL certificates and create required HTTPS binding on the site server computers.
Native 64-bit version of Symantec Management Agent for UNIX and Linux is introduced.	The Symantec Management Agent for UNIX and Linux and all additional plug-ins are now fully 64-bit. The version of the operating system is detected automatically and does not require user involvement.
Task server performance and stability improvements	The following improvements were made in the task server architecture: ■ A Windows Task Scheduler Library **NS.Restore Task Servers** schedule is introduces. It allows the following: Disaster recovery: You can restore Task Server definitions after NS reinstallation or after a new NS database was created. You can add site server definition to a task server, that was manually installed using a distributable package. ■ A separate application pool in IIS for task servers is introduced. ■ IIS7 functionality is now supported in native mode.
Package server performance and user interface improvements.	The following improvements were made in the package server infrastructure: ■ Package server can now be installed on the computers that use IIS 8.5 ■ The user interface for package server was reworked. ■ For Linux package servers, `aex-ps` command line tool is introduced. You can use this tool to manage and monitor package server functionality on a given server.

What's new in ITMS Management Views

In ITMS Management Views 7.5 SP1, the following new features are introduced:

Table 1-3 List of new features

Feature	Description
Computer filter tree is shown in the ITMS Management Views.	The list of computer filters is shown under **Manage > Computers**. The computer filters can be configured and reused. The number of items that are displayed in the tree can be configured.
Easy ways to create new computer filters.	In the ITMS Management Views, new computer filters can be created and configured them in the navigation pane.
An updated list of the default filter criteria.	The following default criteria have been added to the **Add Filter Criteria** list: ■ Asset Status ■ Category (this is a default criteria for software products) ■ Chassis Type ■ OS Revision ■ OS Type ■ Owner ■ System Type
The list of custom criteria.	The option **Edit Criteria List** lets the user add new custom criteria to the filter criteria list. The user can view the values for the associations, data classes, and columns that are selected.
Tthe computer target tree is shown in the ITMS Management Views. create new computer targets, configure, and reuse them.	The list of computer targets is shown under **Manage > Computers**. New computer targets can be created, configure,d and reused. The targets can also be reused in policies and tasks. The number of items that are displayed in the tree can be configured.
Customizable page layout per user.	The user can choose which computer filters or computer targets to display or hide in the **Filters** and **Targets** lists. The list of custom filter criteria, the size of the panes, and the way the elements are displayed on the page can be configured. These settings are saved individually for each user.
Load on-demand feature.	The items in the lists are displayed in chunks. The number of items to be displayed in one chunk can be customized. The rest of the list collapses and is loaded on demand. The load on-demand feature is enabled by default.
Improved drag and drop function and error handling.	After an element is dragged and dropped, a dialog box appears that shows the results of the action.

Table 1-3 List of new features *(continued)*

Feature	Description
Availability of the Management Views.	ITMS Management Views for **Computers**, **Policies**, and **Jobs/Tasks** are available to all users regardless of the installed solutions. The **Software** view is available if there is Software Management Solution and Inventory Solution installed.

What's new in Server Management Suite

The following table lists the new features in the Server Management Suite 7.5 SP1 solutions:

Table 1-4 List of new features in Server Management Suite 7.5 SP1 solutions

Feature	Description

Modification of Integration Component generators	The Integration Component generators are modified to use T4 text templates instead of NVelocity templates.
	To accommodate this change, the following NS6 generators are removed:
	■ Three NS6 pre-created generator projects as follows:
	  ■ Symantec.Components.Generated.Altiris.ASDK
	  ■ Symantec.Components.Generated.Altiris.ASDKTask
	  ■ Symantec.Components.Generated.Altiris.Resource
	■ Reports component generator for NS6 version
	■ Remedy generator
	■ Ensemble generator
	■ Profile service generator

Table 1-4 List of new features in Server Management Suite 7.5 SP1 solutions *(continued)*

Feature	Description
Replacement of SyncFusion library	The SyncFusion libraries are replaced in Workflow Solution. Following are the affected areas: ■ Formula components in `LogicBase.Components.Calc.dll` The **Formula** component and the **Formula Equals Value Rule** component are now replaced with the custom component that implements the following most commonly-used operations: ■ Add ■ Subtract ■ Multiply ■ Divide ■ Average ■ RAND (Random Number) ■ STDEV (Standard Deviation) ■ IRR (Internal Rate of Return) ■ NPV (Net Present Value)

Table 1-4 List of new features in Server Management Suite 7.5 SP1 solutions *(continued)*

Feature	Description
Replacement of SyncFusion library	■ Microsoft Office components Microsoft Office components that were previously found in `LogicBase.Components.Office.dll` are replaced with components built using the Microsoft Software Development Kit (SDK). As a result, only the new file formats `.docx` and `.xlsx` are supported. The `.doc` and `.xls` file formats are no longer supported. Following are the affected **Office** components: ■ Excel Configuration Based Editing (Model) component that includes the following components: ■ Excel Get Action ■ Excel Replace Action ■ Excel Run Macro Action ■ Excel Get Value ■ Excel Replace Value ■ Excel Write ■ Linked Word Merge ■ Word Merge ■ Convert Word To Text ■ Word Model ■ Append Document Action ■ Document Background Action ■ Document Properties Action ■ Insert Break Action ■ Insert Comment Action ■ Insert Footnote Endnote Action ■ Insert Hyperlink Action ■ Insert Image Action ■ Insert List Action ■ Insert Merge Field Action ■ Insert Table Action ■ Insert Text Action ■ Page Numbers Action ■ Replace Text Action ■ **Excel** generator ■ **Script** generator

Table 1-4 List of new features in Server Management Suite 7.5 SP1 solutions *(continued)*

Feature	Description
RapiDeploy tool for imaging computers.	This release onwards, Deployment Solution does not support the RapiDeploy imaging tool. However you can deploy the existing .img images that were created using the RapiDeploy tool.
Deployment Solution plug-in 64-bit Linux is added.	Deployment Solution plug-in for x64 bit for Linux is now added that lets you manage Linux 64-bit client computers.
Windows preboot environment is not packaged with Deployment Solution.	The Windows preboot configuration is no longer packaged with Deployment Solution. To use the WinPE as a preboot environment, you must first download and install the Windows ADK for Windows 8 and then import the Windows ADK to install into Deployment Solution. This activity consumes around 3 hours. ■ Installing ADK takes about 1 hour ■ Creating package takes about 30 minutes ■ Creation of Bootwiz automation package takes about 1 hour

System requirements and supported platforms

Before you install Server Management Suite 7.5 SP1, read the section Hardware recommendation in the *IT Management Suite 7.5 SP1 Planning for Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC7332

For any additional solution and components system requirements, see the chapters for individual solutions in this document.

For information about the supported operating systems in Symantec Management Platform 7.5 SP1 and the IT Management Suite 7.5 SP1 solutions, see the article in the following URL:

http://www.symantec.com/docs/HOWTO9965

General installation and upgrade information

Use Symantec Installation Manager to install Symantec Management Platform (SMP) 7.5 SP1 and the Server Management Suite (SMS) 7.5 SP1 solutions.

For more information about Symantec Installation Manager, see the Symantec Installation Manager Getting Started Guide at the following URL:

http://www.symantec.com/docs/DOC6717

The types of installation requirements that you can use based on your current setup are as follows:

- Installation of Symantec Management Platform 7.5 SP1 and the Server Management Suite 7.5 SP1 solutions
- Upgrade to Symantec Management Platform 7.5 SP1 and the Server Management Suite 7.5 SP1 solutions
- Post upgrade versions of Symantec Management Agent and solution plug-ins
- Migration of Notification Server data from a Windows Server 2008 R2 computer to a Windows Server 2012 R2 computer
- Migration to Symantec Management Platform 7.5 SP1 and the Server Management Suite 7.5 SP1 solutions

Installation of Symantec Management Platform 7.5 SP1 and the Server Management Suite 7.5 SP1 solutions

You can download the installation files directly to your server or you can create offline installation packages.

For more information on how to install and configure the product, see the Installing the IT Management Suite solutions chapter in the *IT Management Suite 7.5 SP1 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC6847

Before you install or upgrade Server Management Suite, Symantec Management Platform, or IT Management Suite, ensure that you have reviewed the latest changes to the Symantec Management Platform of this release. For more information on what's new in Symantec Management Platform 7.5 SP1, see the *Symantec™ Management Platform 7.5 SP1 Release Notes* at http://www.symantec.com/docs/DOC7310

Upgrade to Symantec Management Platform 7.5 SP1 and the Server Management Suite 7.5 SP1 solutions

Use Symantec Installation Manager to upgrade to Symantec Management Platform (SMP) 7.5 SP1 and the Server Management Suite (SMS) 7.5 SP1 solutions.

The supported upgrade paths are as follows:

- 7.1 SP2 MP 1.1
  This contains the SMP build version 7.1.8401

- 7.5 HF6
  This contains the SMP build version 7.5.1676

To perform an upgrade from Server Management Suite 7.1 solutions or later, in the Symantec Installation Manager click **Upgrade installed products**, and then choose to install this product.

Symantec recommends that you upgrade all the installed products to the latest version. The easiest way to upgrade to 7.5 SP1 version is to choose to install a suite. If you use hierarchy, you must disable hierarchy replication and upgrade all products to the latest version on each of the Notification Server computers.

For more information on how to upgrade to Server Management Suite 7.5 SP1 solutions, see the Upgrading to IT Management Suite 7.5 SP1 chapter in the *IT Management Suite 7.5 SP1 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC6847

Upgrade the Symantec Management Agent, site servers, and solution plug-ins

After upgrade to Symantec Management Platform 7.5 SP1, you can upgrade the Symantec Management Agent (SMA) on client computers to SMA 7.5 SP1. Additionally, you must upgrade the solution plug-ins to the latest versions that are available in SMP 7.5 SP1 and SMS 7.5 SP1. An older version of SMA can communicate with a latest version of SMP using the Legacy Agent Communication (LAC) mode, but Symantec recommends that you upgrade the SMA and the solution plug-ins to the latest version.

To upgrade the Symantec Management Agent, site servers, and solution plug-ins, complete the following tasks in the given order:

1. In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent.
2. In the Symantec Management Console, click **Settings > All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins.
3. In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the upgrade policies for various plug-ins.

Symantec recommends that you configure a schedule for these policies; the default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. Also, to speed up the upgrade process, consider temporarily

changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

Post upgrade versions of Symantec Management Agent and solution plug-ins

The Symantec Management Agent and the solution plug-in versions after you upgrade to ITMS 7.5 SP1 are as follows:

Table 1-5 SMA and plug-in versions after upgrading to ITMS 7.5 SP1

Agent or plug-in	Upgraded version in ITMS 7.5 SP1
Symantec Management Agent	7.5.3153
Altiris Client Task Agent	7.5.3153
Altiris Client Task Server Agent	7.5.3153
Altiris Base Task Handlers	7.5.3153
Deployment Task Server Handler	7.5.3219
Deployment Package Server	7.5.3219
Software Management Framework Agent	7.5.3153
Software Management Solution Agent	7.5.3219
Virtual Machine Management Task Handler	7.5.3219
Deployment Plug-in for Windows (x86)	7.5.3219
Deployment Plug-in for Windows (x64)	7.5.3219
Deployment Plug-in for Linux (x86)	7.5.3219
Deployment Plug-in for Mac	7.5.3219
Deployment NBS plug-in	7.5.3219
ULM Agent	7.5.3153
Inventory Agent	7.5.3219
Monitor	7.5.3219

Migration of Notification Server data from a Windows Server 2008 R2 computer to a Windows Server 2012 R2 computer

The following table enlists the scenarios for migration of Notification Server data from a Windows Server 2008 R2 computer to a Windows Server 2012 R2 computer:

Table 1-6 Scenarios for migration of Notification Server data to a Windows Server 2012 R2 computer

Scenario	Prerequisite	Migration overview
Migrating Notification Server data to a Windows Server 2012 R2 computer with SQL 2012 as the database.	Install Server Management Suite 7.5 SP1 on a new computer with Windows Server 2012 R2 and SQL 2012 as the database.	■ Back up the Configuration Management Database (CMDB) and create a data store file using the migration wizard on the computer with Windows Server 2008 R2. ■ For some Server Management Suite solutions, you must manually copy the earlier data to a secure backup location. ■ On the new computer with IT Management Suite 7.5 SP1 and Windows Server 2012 R2 with SQL 2012 as the database, restore CMDB, import the data store file, and if required, save the manually copied data.
Migrating Notification Server data to a Windows Server 2012 R2 computer and reusing SQL 2008 as the database.	Install Server Management Suite 7.5 SP1 on a new server that has Windows Server 2012 R2 and connect to the SQL 2008 database.	■ Create a data store file using the migration wizard on the computer with Windows Server 2008 R2. ■ For some Server Management Suite solutions, you must manually copy the earlier data to a secure backup location. ■ On the new computer with IT Management Suite 7.5 SP1 and Windows Server 2012 R2 with reused SQL 2008 database, import the data store file, and if required, save the manually copied data.

For more information on the migration process, see the Migrating Notification Server data from Windows Server 2008 R2 to Windows Server 2012 R2 topic in the *IT Management Suite 7.5 SP1 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC6847

Migration to Symantec Management Platform 7.5 SP1 and the Server Management Suite 7.5 SP1 solutions

If you use Notification Server 6.x or IT Management Suite 7.0 and want to migrate to Symantec Management Platform 7.5 SP1 and Server Management Suite 7.5 SP1, you can use either of the following paths:

- Migrate from Notification Server 6.x or IT Management Suite 7.0 to IT Management Suite 7.1 SP2 and then first upgrade to ITMS 7.1 SP2 MP1.1 followed by the upgrade to ITMS 7.5 SP1.

- Migrate from Notification Server 6.x or IT Management Suite 7.0 to IT Management Suite 7.5 and then first upgrade to ITMS 7.5 HF6 followed by the upgrade to ITMS 7.5 SP1.

For detailed instructions on migrating from Notification Server 6.x or IT Management Suite 7.0 to IT Management Suite 7.1 SP2, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP2* at the following URL:
  http://www.symantec.com/docs/DOC4742
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at the following URL:
  http://www.symantec.com/docs/DOC4743

For detailed instructions on migrating from Notification Server 6.x or IT Management Suite 7.0 to IT Management Suite 7.5, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.5* at the following URL:
  http://www.symantec.com/docs/DOC5668
- *IT Management Suite Migration Guide version 7.0 to 7.5* at the following URL:
  http://www.symantec.com/docs/DOC5669

For detailed instructions on migrating Notifications Server from a Windows Server 2008 R2 computer to Notifications Server 7.5 SP1 on a Windows Server 2012 R2 computer, see the Migrating Notification Server data from Windows Server 2008 R2 to Windows Server 2012 R2 topic in the *IT Management Suite 7.5 SP1 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC6847

For detailed instructions on upgrading from IT Management Suite 7.1 SP2 or 7.5 to IT Management Suite 7.5 SP1, see the Upgrading to IT Management Suite 7.5 SP1 chapter in the IT Management Suite 7.5 SP1 Installation and Upgrade Guide at the following URL:

http://www.symantec.com/docs/DOC6847

Other things to know

The following are the things to know about this release. If additional information about an item or feature is available, a corresponding article link is provided.

Table 1-7 Other things to know

Issue	Description	Article link
SymHelp access with IE 8, IE 9 or later.	When SymHelp contains the content that can be accessed through HTTP or HTTPS protocols, by default, the Internet Explorer displays only secured content, thereby blocking all unsecured content. To let Internet Explorer display the blocked SymHelp content, do the following: ■ Go to your browser security settings and customize it to enable the mixed content display.	kb/2625928 ee264315

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-8 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Release Notes**.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Table 1-8 Documentation resources *(continued)*

Document	Description	Location
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ Click the page and then press the F1 key. ■ Use the Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-9 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase
Cloud Symantec Help Center	All available IT Management Suite and solution guides are accessible from this Symantec Help Center that is launched on cloud.	http://help.symantec.com/CS?locale=EN_US&vid=v90719369_v93032876&ProdId=SYMHELPHOME&context=itms7.5

Table 1-9 Symantec product information resources *(continued)*

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management/forums/endpoint-management-documentation Here is the list of links to various groups on Connect: ■ Deployment and Imaging http://www.symantec.com/connect/groups/deployment-and-imaging ■ Discovery and Inventory http://www.symantec.com/connect/groups/discovery-and-inventory ■ ITMS Administrator http://www.symantec.com/connect/groups/itms-administrator ■ Mac Management http://www.symantec.com/connect/groups/mac-management ■ Monitor Solution and Server Health http://www.symantec.com/connect/groups/monitor-solution-and-server-health ■ Patch Management http://www.symantec.com/connect/groups/patch-management ■ Reporting http://www.symantec.com/connect/groups/reporting ■ ServiceDesk and Workflow http://www.symantec.com/connect/workflow-servicedesk ■ Software Management http://www.symantec.com/connect/groups/software-management ■ Server Management http://www.symantec.com/connect/groups/server-management ■ Workspace Virtualization and Streaming http://www.symantec.com/connect/groups/workspace-virtualization-and-streaming

Chapter 2

Deployment Solution

This chapter includes the following topics:

- What's new in Deployment Solution
- Known Issues
- Fixed Issues

What's new in Deployment Solution

In Deployment Solution 7.5 SP1, the following new features are introduced:

Table 2-1 List of new features in Deployment Solution 7.5 SP1

Feature	Description
Windows preboot environment is not packaged with Deployment Solution.	The Windows preboot configuration is no longer packaged with Deployment Solution. To use the WinPE as a preboot environment, you must first download and install the Windows ADK for Windows 8 and then import the Windows ADK to install into Deployment Solution. This activity consumes around 3 hours. ■ Installing ADK takes about 1 hour ■ Creating package takes about 30 minutes ■ Creation of Bootwiz automation package takes about 1 hour
Deployment Solution plug-in 64-bit Linux is added.	Deployment Solution plug-in for x64 bit for Linux is now added that lets you manage Linux 64-bit client computers.

Table 2-1 List of new features in Deployment Solution 7.5 SP1 *(continued)*

Feature	Description
RapiDeploy tool for imaging computers.	This release onwards, Deployment Solution does not support the RapiDeploy imaging tool. However you can deploy the existing .img images that were created using the RapiDeploy tool. **Note:** When you upgrade from IT Management Suite 7.1 SP1 MP1.1 or from IT Management Suite 7.5 HF6 to IT Management Suite 7.5 SP1, you must edit the tasks and jobs that contain the **Create Image** task using RapiDeploy imaging tool to **Create Image** task using the Ghost imaging tool. For more information refer to the Symantec™ IT Management Suite 7.5 SP1 powered by Altiris™ technology Installation and Upgrade Guide.

Known Issues

The following are the known issues for this release:

Table 2-2 Known Issues of Deployment Solution

Issue	Description	Article Link
Multiple NIC entries cannot be added for a predefined computer.	You cannot specify multiple NIC entries when adding a predefined computer through the **Predefined Computers** dialog box of the console. The workaround to this issue is that you can add one NIC as DHCP and the other NICs as static.	N/A
For Mac computers, the **Apply System Configuration** task is not able to restore the network details.	For Mac computers, you cannot restore the network details such as Domain suffix using the restore functionality of the **Apply System Configuration** task. You can modify only the host name using the **Apply System Configuration** task.	N/A
New drivers do not replicate on package server computer if exception is thrown during addition of drivers.	During addition of drivers through the **Driver Database Management** dialog box, if an exception is thrown, then the new drivers are not replicated on the package server computer. The workaround to this issue is that after you get an exception on the driver management console, import only a single driver which displays the result of the addition of driver in the console. Later, you can find the other drivers replicate on the Package server.	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
A predefined computer with a space in the UUID hardware identifier boots as an unknown computer.	If the UUID hardware identifier of a predefined computer has a space separator, then it boots as an unknown computer after you add the computer into the network	N/A
You cannot install the Network Boot Service on a Windows 8.1 computer.	You cannot install the Network Boot Service on a Windows 8.1 computer as the Network File System (NFS) service is not listed in a Windows 8.1 computer.	N/A
The Domain Administrator Password is displayed in the unattend.xml answer file.	The Domain Administrator Password is displayed in the unattend.xml answer file after you execute the following tasks using the Sysprep: ■ **Prepare for Image Capture** task ■ **Create Image** task	N/A
For a Linux predefined computer, deployment of Sysprep image does not retain the predefined name.	For a Linux predefined computer, deployment of a Sysprep image does not retain the name of the predefined computer.	N/A
If image creation operation stops in middle, Ghost tool re-launches and continues to create image over UNC path.	While creating images using the Ghost imaging tool, image creation task stops in the middle, the Ghost tool launches again, and the image creation again continues over the UNC path	N/A
The **Apply System Configuration** task fails to change the host name for the SUSE Linux Enterprise SP1 client computers.	You cannot change the host name for the SUSE Linux Enterprise SP1 client computers through the **Apply System Configuration** task.	N/A
For Mac OS X 10.6 version, the running application icons are not displayed in the dock of the client computer that is booted into the automation environment	For Mac OS X 10.6 version, the running applications are not captured during automation partition creation. When the client computer is booted in the automation environment using the automation folder, the running application icons are not displayed.	N/A
The **Install Windows OS** task fails in a Notification Server only set-up.	The **Install Windows OS** task fails in a Notification Server only set-up if the port 445 is blocked.	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
The **Erase Disk** task status displays as failed in the console even when the task is executed successfully.	The **Erase Disk** task displays the status as failed even when the task is executed successfully. This issue occurs when you execute the task to erase a disk of a client computer that has multiple disks and different operating systems installed on the disks.	N/A
You cannot recreate the PEInstall and LinInstall configuration with the **Repair** option of the Symantec Installation Manager.	You cannot recreate the PEInstall and LinInstall configuration with the **Repair** option of the Symantec Installation Manager. This issue occurs when you delete the configuration files from the following paths and recreate the PEInstall with the **Repair** option from the Symantec Installation Manager: ■ <Install_dir>:\Program Files\Altiris\Notification Server \NSCap\bin\Win32\X86\Deployment\Automation\ PEInstall_x86 ■ <Install_dir>\Program Files\Altiris\Notification Server \NSCap\bin\Win64\X64\Deployment\Automation\ PEInstall_x64 ■ <Install_dir>:\Program Files\Altiris\Notification Server\NSCap\bin\UNIX\ Deployment\Linux\x86\Automation\LinInstall_x86 Following is the workaround for this issue: In the Symantec Management Console, navigate to **Setting > Deployment > Create Preboot Configurations**, select the PEInstall or LinInstall, and click the **Recreate Preboot Environment**.	N/A
A UEFI-based computer is unable to boot to production when deploying a BIOS-based Windows 8 64-bit image.	A UEFI-based computer with secure boot mode enabled is unable to boot to production when deploying a BIOS-based Windows 8 64-bit image.	N/A
For 10.9 OS X, the **Deploy Image** task fails.	For 10.9 OS X, the **Deploy Image** task fails when the **Resize Partition** option is set to **Proportionately** and the size of the source disk is equal to the target disk size.	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
Failed to boot the client computer with 10.9 OS X NetBoot image that is created from the Temp volume or the DSAutomation folder.	Failed to boot the client computer with 10.9 OS X NetBoot image that is created from the Temp volume or the DSAutomation folder. The following error is displayed: Unapproved caller: securityagent may only be invoked by Apple software. Following is the workaround for this issue: Install the MOCU app in a bootable volume and select the bootable volume on which Symantec Management Agent and the Deployment Solution plug-in for Mac are installed as the source volume for creating the NetBoot image	N/A
The NFS shared path is not enabled for a Windows Server 2008 SP2 Network Boot Service (NBS) computer.	The NFS shared path is not enabled for the MacNetShare folder, even when the NFS service is installed for a Windows Server 2008 SP2 NBS computer.	N/A
For Linux computers, the **Boot To** task when executed displays incorrect status.	For Linux, the client computers that are booted in the production environment, the **Boot To** task status displays as Failed even after the task completes successfully.	N/A
In the **Deploy Image** task, the UNC path is displayed for the images.	The **Deploy Image** task displays a UNC path for the images that are created using the HTTP path or the HTTPS path.	N/A
An external hard disk that is connected to the package server computer is considered as a fixed drive and the package share is created on the connected external hard disk.	An external hard disk that is connected to the package server computer is considered as a fixed drive and the package share is created on the connected external hard disk.	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
Undefined error occurs on SMP and **Personality Capture** task fails if client computer moves to non-CEM mode.	An undefined error occurs on the SMP and the **Personality Capture** task fails if CEM policy is enabled. After the CEM policy is enabled, the package servers that are in the non-CEM environment are also CEM enabled and the client computer of the non-CEM environment fails to communicate with the package servers The workaround to this issue is as follows: ■ Go to **Settings > Notification Server > Cloud-enabled Management** ■ Expand **Policy > Cloud-enabled Management Settings** ■ Select the **Applied To filter > Click Edit** (Pencil icon) ■ Click **Update results** ■ Right-click on the Package server which is expected to be in the **Non-CEM environment > Click Exclude > Click OK** ■ Click **Save Changes.** After the non-CEM package servers are removed from the CEM policy, the status on the package server changes to CEM disabled. The non-CEM client computers can then communicate with the non-CEM package server.	N/A
For Mac computers, saved data for the network adapter is not displayed in the **Apply System Configuration** task.	For Mac computers, when you create an **Apply System Configuration** task, if you set the DNS1 address as `Leave existing` and provide only DNS2 address, then the DNS2 address is not saved and is not available in the **Edit configuration…** of the **Apply System Configuration** task for editing.	N/A
A Linux image that is created over HTTP and imported using Resource Import tool does not display partition details in the **Advanced** tab of the **Deploy Image** task dialog box.	For Linux client computers, the partition information is not displayed in the **Advanced** tab of the **Deploy Image** task for an image that is created over HTTP and is imported using the Resource Import tool.	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
The **Create Image** task fails when the default drive on package server is full.	The **Create Image** task fails to create new images when the default drive on the package server is full. The workaround for the issue is as follows: In the Symantec Management Console, create a **Copy File** task that replicates a package that is created on Notification Server to the package server. This replication of the package creates a new net share on the package server if an additional drive is available on package server.	N/A
If Package Server is in HTTPS mode, then **Install Windows OS** task fails with error.	The following error message is displayed and the **Install Windows OS** task fails if the package server is launched in HTTPS mode: `Package Path is Null`	N/A
Ghost imaging tool attempts multiple times to create image on web server even when the server is unavailable.	Even when the web server is unavailable, the Ghost imaging tool attempts multiple times to create an image on the web server from the client computer.	N/A
Restore Backup Image task fails if image is stored in non-default path.	The **Restore Backup Image** task fails if the image package is stored in the non-default location of the computer.	N/A
For Mac, the **Deploy Image** task fail that involves deploying image of a non-HFS or HFS type of disk partition when the DS Automation volume is located with the target volume on the same disk	For Mac, the **Deploy Image** task fails to deploy an image for the following if the DS Automation volume is located with the target volume on the same disk and the client computer is booted in the preboot environment using the DS Automation volume ■ An image of a non- HFS type of disk partition is deployed on a disk that has HFS type of partition. ■ An image of an HFS type of disk partition is deployed on a disk that has non-HFS type of partition.	N/A
Support issue related to the **Install Linux/ESX OS** task.	The **Install Linux/ESX OS** task is not supported for RHEL 6.2 and RHEL 6.3 version.	N/A
The **Deploy Image** task cannot be stopped by using the stop option of the task status page of the Symantec Management Console.	You cannot stop the execution of the **Deploy Image** task on the client computer from the task status page of the Symantec Management Console.	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
The 32-bit virtual machine or the ESX client computers cannot boot into preboot environment using WinPE4.0.	You cannot boot a 32-bit virtual machine or an ESX client computer into preboot environment using WinPE4.0 For more information on this issue refer to the following: ■ VMware Community ■ Microsoft TechNet	N/A
For Mac, the Automation folder install policy fails to download the automation folder on the client computer when the thumbs.db file is present in the Automation folder or the Agent folder	For Mac, the Automation folder install policy fails to download the automation folder on the client computer if the thumbs.db file is present as hidden in the Automation folder or the Agent folder A thumbs.db file is generated when you access the Automation folder or the Agent folder from the <Install_dir>\Program Files\Notification Server\NSCapBin\ UNIX\Deployment\Mac\universal\ path and change the view of the folder content to Thumbnails view Following is the workaround for this issue: ■ Navigate to <Install_dir>\Program Files\Notification Server\NSCapBin\ UNIX\Deployment\Mac\universal\Automation folder ■ Select Show hidden files, folder, and drives. ■ Uncheck the Hide Protected operating system files(Recommended) check box ■ If the Thumbs.db file is present then run the following command in the command prompt for the location where the file is generated (with Administrator Privileges `ATTRIB -S -H Thumbs.db`	N/A
The **Copy File** task fails and displays an error message when you copy a file on the client computer that is booted in the automation environment.	The **Copy File** task fails when you copy a file of size that is equal to or greater than half the size of the RAM disk of the client computer that is booted in the automation environment when enough space is available on the X drive and displays the following error message `Not enough space available on the destination drive.` Following is the workaround for the issue: Use the **Run Script** task to map the drive on which the file is located and then use the file when the client computer is booted in the preboot environment	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
Client computer does not join the domain after executing the **Deploy Image** task.	Client computer does not join the domain after executing the **Deploy Image** task for the following operating systems: ■ Windows 8 ■ Windows 8.1 ■ Windows Server 2012 R2 Following is the workaround for this issue: Execute the **Apply System Configuration** task for the computer to join a domain.	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link

The **Prepare for Image capture** task fails on a computer that is installed with Windows 8.1.	The **Prepare for Image capture** task fails on the client computer that is installed with Windows 8.1.
	Apply one of the following workarounds:
	Workaround 1
	■ Create an Admin user with Administrator privileges other than the domain user of the client computer.
	■ Log in to the client computer as the Local computer Administrator.
	■ Execute the **Prepare for Image capture** task on the client computer.
	If the domain join fails, use the Apply System Configuration task to join the client computer to the domain.
	Workaround 2
	■ Log in to the computer with an Administrator account or Run Windows PowerShell as an Administrator.
	■ Execute the following command in PowerShell:
	`Get-AppxPackage -AllUser | Where PublisherId -eq 8wekyb3d8bbwe`
	The command generates the list of packages that are installed for the users.
	From the list of packages, delete the additional packages that are installed only for the local Administrator and not for the domain user.
	Use the following command to delete the additional packages:
	`Remove-AppxPackage -Package <packagefullname>`
	■ Log in to the computer from the domain user and execute the **Prepare for Image capture** task.
	For more information refer to the following URL:
	http://support.microsoft.com/kb/2769827
		kb/2769827

For RHEL5.10, the computer does not boot in the production environment.	For RHEL5.10, the computer does not boot in the production environment after you deploy an image that is created using the RapiDeploy tool.	N/A

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
For ESXi 5.5, the **Install Linux/ESX OS** task fails.	For ESXi 5.5, the **Install Linux/ESX OS** task fails. Following is the workaround for this issue: ■ In the operating system package delete the LSI_MR3.V00. ■ Create a copy of LSI_MSGP.V00 and rename it as LSI_MR3.V00 in the operating system package.	N/A
The **Create Image** task fails to create image over the HTTP path.	The **Create Image** task fails to create image over the HTTP path if the credentials that are provided while installing the Symantec Management Platform and the domain credentials are not entered in the same case	N/A
Drivers are not installed for a Windows Server 2008 x86 computer.	The drivers are not installed for a Windows Server 2008 x86 computer after you execute the Install Windows OS task with Deploy Anywhere as there are compatibility issue between Windows Server 2008 and WinPE 4.0.	http://social.technet.microsoft.com/
The **Create Image** task fails to create image if the IT Management Suite is installed as a Local Administrator.	The **Create Image** task fails to create image if the IT Management Suite is installed with Local Administrator credentials on a computer that is added in the domain Following is the workaround for this issue: ■ On the Package server, in the IIS manager, disable the Digest Authentication and enable the Basic Authentication.	N/A
An error is displayed while uninstalling the NBS service from a site server.	When you uninstall the NBS (x86) service from a site server the error code 1605 is displayed as follows: This action is only valid for the products that are currently installed.	N/A
The Power Control tasks are not executed when the client computer is booted in the preboot environment.	The Power Control tasks are not executed when the client computer is booted in the preboot environment. Following is the workaround for this issue: ■ To shut down a computer that is booted with WinPE, use the Run Script command with `shutdown -s -f -t 5`. ■ To shut down a computer that is booted with the LinuxPE, use the Run Script command with `shutdown -s now /y`. ■ To boot a computer in production environment use the **Boot To** task.	TECH211551

Table 2-2 Known Issues of Deployment Solution *(continued)*

Issue	Description	Article Link
The **Boot To** task displays incorrect task status.	The **Boot To** task status displays failure on the console even when the task is executed successfully on the client computer when you execute the task in a job to deploy an image that was captured using ITMS 7.1 SP2 MP1.1. Following is the workaround for this issue: To execute the tasks that are scheduled after executing the **Boot To** production task, uncheck the **Fail job if any task fails** option of the job.	N/A

The **Deploy Image** task fails with critical error.	The Deploy Image task that uses custom unattended Sysprep files fails and displays the following error:
	`A critical error has occured on this page. Check the Altiris log for more information.`
	This error occurs when you upgrade from ITMS 7.5 HF6 or ITMS 7.1 SP2. The
	Following are the workarounds for this issue:
	Workaround 1
	■ Before you upgrade to ITMS 7.5 SP1
	Create your own custom folder in Deployment share, back-up, and store all your custom Sysprep and other files on Notification Server.
	For example:
	`<instal_dir>\NSCap\bin\Win32\X86\Deployment\MyFiles\`
	Workaround 2
	■ After you upgrade to ITMS 7.5 SP1 and the custom answer files are deleted
	You must restore or re-create the custom files and place them back in the Deployment folder root.
	■ Run following SQL query to fix the corrupted database which is caused by the missing files.
	`UPDATE ItemVersionData SET [State] = cast([State] as nvarchar(max)) + '</vItem>' WHERE [State] like '<vItem>%' and [State] not like '%</vItem>' and LEN(cast ([State] as nvarchar(max))) < 4000`
	■ Edit the task or the job that uses the custom files and modify the task so that the task or the job is recreated in the database.
		TECH218252

Fixed Issues

Following is the list of Fixed issues in this release

Table 2-3 Fixed Issues of Deployment Solution

Issue	Description	Article link
The system time of the computer displays incorrect time.	After you deploy an image, the system time of the computer displays incorrect time.	N/A
You cannot change the **Command Line** option of a **Copy File** task.	You cannot change the **Command Line** option of a **Copy File** task when you assign it to a computer.	N/A
The **Copy File** task fails to execute.	The **Copy File** task fails to execute the task if the file that is copied from the source computer exists on the destination computer.	N/A
A job fails to execute when a predefined computer record is merged.	A job fails to execute when a predefined computer record is merged when the computer is imported using the Active Directory Import.	N/A
The automation folder is not updated on the client computers after you recreate the preboot configuration.	The automation folder is not updated on the client computers. After you update the preboot configuration the package distribution points are not updated after you recreate the preboot configuration.	N/A
The driver database is not updated on the site servers after you add drivers to the database.	The driver database is not updated on the site servers after you add drivers to the database. After you update the preboot configuration the driver database is not updated after you recreate the preboot configuration.	N/A
An unknown computer that is booted in the preboot environment fails to execute any software delivery task.	You cannot execute any software delivery task on an unknown computer that is booted in the preboot environment using the default response that is set for unknown computers or by using the F8 key.	N/A
Incorrect help opens when you click on the help icon of the **Partition Disk** task.	The help icon that is present on the **Partition Disk** task does not open relevant help when you use the Internet Explorer 9 browser to browse the console.	N/A
Cannot add more than one predefined computer.	More than one predefined computers are not added through the **Add Predefined Computer Settings** page.	TECH217886

Chapter 3

Inventory Solution

This chapter includes the following topics:

- Known issues
- Fixed issues
- Other things to know

Known issues

The following are the known issues for this release.

The known issues are separated into the following groups:

- Installation and upgrade issues.
  See Table 3-1 on page 44.
- Hierarchy and replication issues.
  See Table 3-2 on page 44.
- Other known issues that are common for all types of platforms.
  See Table 3-3 on page 44.
- Other known issues for Windows platforms.
  See Table 3-4 on page 46.
- Other known issues for UNIX, Linux, and Mac platforms.
  See Table 3-5 on page 47.
- Known issues for Inventory Pack for Servers.
  See Table 3-6 on page 54.

Table 3-1 Installation and upgrade issues

Issue	Description	Article link
After upgrade to 7.5 SP1 you need to upgrade Inventory Plug-in.	After you upgrade the Symantec Management Agent to 7.5 SP1 version, the Inventory Plug-in does not function until you upgrade it to 7.5 SP1	N/A

Table 3-2 Hierarchy and replication issues

Issue	Description	Article link
Replicated custom data class is editable on a child Notification Server computer.	When you create a custom data class, and then replicate the data class from the parent Notification Server computer to its child, the custom data class is editable on the child Notification Server computer A custom data class that is defined on the parent Notification Server computer should never be editable on a child Notification Server computer.	N/A
Different region time format settings on parent and child servers lead to incorrect **Days Metered** data display.	If the parent Notification Server and child Notification Server have different region time format settings, the **Days Metered** count on the **Underutilized Software** report page displays incorrect value.	N/A
When you replicate a task from parent to child NS, the task advance options can be edited.	When you replicate an inventory task from a parent Notification Server to a child Notification Server in a hierarchy, you can edit the advanced options of the replicated task on the child NS computer. After you edit the advanced options of the replicated task on the child NS computer and click **Save changes**, the changes that you made are not saved. Normally, the advanced settings on the replicated task page should not be editable, and the Save changes and Cancel buttons should not be enabled.	N/A

Table 3-3 Other known issues that are common for all types of platforms

Issue	Description	Article link
Inventory scan returns incorrect value for the **HW Baseboard** data class.	When you run an inventory scan on Mac or Windows client computers, the scan returns an incorrect value for the **HW Baseboard** data class.	N/A

Table 3-3 Other known issues that are common for all types of platforms *(continued)*

Issue	Description	Article link
Inventory install, uninstall, and upgrade policies do not run once ASAP in the maintenance window only.	You can check **Run once ASAP** on a policy page to run inventory install, uninstall, and upgrade policies once as soon as possible. However, you cannot currently run the policies once ASAP in the maintenance window only.	N/A
Incorrect Install Date in inventory reports.	Inventory reports display incorrect Install Date for installed software products.	TECH133481
File inventory is not collected for some software components. As a result, you cannot meter the usage of these software components.	During full inventory scan, file inventory is not collected for the software components that are not .MSI based. You cannot view file inventory data when you right-click a non-MSI based software component, click **Actions > Edit Software Resource**, and then click the **File Inventory** tab. As a result, you cannot automatically meter the usage of this software component as it has no file inventory and is not associated with an executable file. To enable a non-MSI based software component for metering, you should manually add executable files to the software component. For more information, see the topics about association of new program files to metered software components in the *Inventory Solution 7.5 SP1 User Guide*. http://www.symantec.com/docs/DOC7217	N/A
A license is not reclaimed when the **Asset Status** is set to a custom asset status.	A license is not reclaimed when the **Asset Status** is set to a custom asset status. Inventory Solution license should be reclaimed on setting the **Asset Status** to other than **Active**.	N/A
If you create several rules for the same type of files, the delta inventory information is not sent for those files.	When you create an Inventory policy to gather the information about file properties and, in the **Advanced Options** dialog box, create several rules for the same file type, the S**end inventory changes (deltas)** only does not work for that type of files. Full information is sent to the Notification Server computer after each inventory scan.	N/A

Table 3-4 Other known issues for Windows platforms

Issue	Description	Article link
When you use Internet Explorer 10 or 11 to download a stand-alone package, an error occurs.	When you try to download a stand-alone package from the Notification Server computer through the links available on the Symantec Management Console, an error message is displayed, saying that the publisher of the program cannot be verified. This issue occurs if you use Internet Explorer 10 or 11, because of the **SmartScreen Filter** security feature by Microsoft. You can directly download the package exe from the `NSCap` folder on the server, and run it on unmanaged client computers.	N/A
After the NS.Nightly schedule task runs, the Yahoo! Messenger is displayed in the Software Catalog under **Newly Discovered Software** instead of under **Unmanaged Software**	After you gather inventory, the data about Yahoo! Messenger is not displayed in the Software Catalog. This happens because Software Management Framework is unable to gather the information about the version of this product. After you run the NS.Nightly schedule task, the Yahoo! Messenger is displayed on the **Software Catalog** page, under **Newly Discovered Software** instead of under **Unmanaged Software**.	N/A
File scan unable to gather the data if the file type is written in capital letters.	When you configure the advanced options for the Inventory policy and include a file scanning rule for a file type that is not in a default list, the files are not scanned if the file type is written in capital letters.	N/A
Data class information is missing because Microsoft IIS version 8.0 drops some registry key.	When you view the data class information in the Resource Manager, on the **IIS Settings** page, the values for some fields are not populated. This happens because Microsoft IIS version 8.0 drops some registry keys and Inventory Solution cannot report inventory for these fields.	N/A
A huge number of events is logged into the SMA log during software scan on Windows 8 computers.	When you run a software scan on a Windows 8 computer with trace level logging enabled, numerous events are logged into the Symantec Management Agent (SMA) log. As a result, the SMA log folder size can exceed 1GB. To avoid this issue, disable trace level logging before you run the software scan.	N/A

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms

Issue	Description	Article link
Altiris_HW_Baseboard inventory reports incorrect value data for Mac client client computers.	Altiris_HW_Baseboard inventory reports incorrect value data for Mac client client computers. The following fields report incorrect value: ■ Altiris_HW_Baseboard.SerialNumber=Base Board Serial# ■ Altiris_HW_Baseboard.Version=Proto1	N/A
Inventory does not report the core count.	Processor data class inventory does not report individual CPU core information.	N/A
`.Trash` directories must be excluded from a software inventory scan by default when you run the scan on Mac, UNIX, or Linux computers.	If an application is deleted, it is moved to the `<userhome>/.Trash` directory. `.Trash` directories must be excluded from a software scan by default; however currently they are presented in the software scan results. When you run a software inventory scan, you have to manually exclude the `.Trash` and `.Spotlight-V100` folders on the Mac platform and the `.Trash` folder if it exists on UNIX or Linux platforms.	N/A
On UNIX and Linux computers, an inventory task keeps running permanently during the software inventory scan on a directory with a large number of items.	When you run software inventory using the `filescan.rule` file on a directory with an extraordinary large number of items, the `swscan.bin` gets completed but the inventory task keeps running permanently and no NSE file is generated. As a workaround, you can use folder or file scanning limitations to reduce the number of scanned items.	N/A
The SoftwareScanner does not scan "~" (home directory).	The SoftwareScanner does not process the "**~**" home directory by the rule: `<folder status="include" scanSubFolders="true">~</folder><folderLimits />`	N/A
Inventory task execution on UNIX, Linux, and Mac computers.	When you run software inventory, it is possible to run three inventory tasks simultaneously on UNIX, Linux, and Mac computers. Running three software inventory tasks at the same time results in the system overload and long execution time because CPU usage increases to 100%. As a workaround, you can schedule the tasks to avoid running them simultaneously.	N/A

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description	Article link
On UNIX, Linux, and Mac computers, inventory data is not sent after Inventory Plug-in is redirected to another Notification Server computer and delta inventory is enabled in an inventory task.	After you run some inventory task with delta inventory enabled on one Notification Server computer, redirect Inventory Plug-in to another Notification Server computer, and run another inventory task with delta inventory enabled along with some other types of inventory, only delta inventory data is sent.	N/A
On UNIX, Linux, and Mac computers, **OS_NFSShare** gets incorrect results if `/etc/exports` contains invalid records.	According to the logic of script, **nfstat** lets you figure out active calls and `/etc/exports` provides you with share points. If `/etc/exports` contains an incorrect entry, the **OS_NFSShare** output gets incorrect results. The system utility `exportfs` controls incorrect entries and filters them when share points are created and listed.	N/A
The **UG_UserUsage** script does not detect local login on Solaris platforms.	The **UG_UserUsage** script does not detect entries for any local logins on Solaris platforms.	N/A
On UNIX, Linux, and Mac computers, NSE file contains unchanged data after software inventory scan, even if delta inventory is enabled.	When you collect software inventory using the filescan rules with delta inventory enabled for the second time, NSE file contains full inventory data. However, it should contain only the changes in the target directory such as changed number or size of files.	N/A
Some values of the **OS_Timezone** data class are reported incorrectly or not reported on HP-UX platforms.	If the time zone is not GMT, the values of the **OS_Timezone** data class are reported incorrectly or not reported on HP-UX platforms. The **StandardName, StandardCaption, StandardOffset** values are reported incorrectly. The **DaylightName, DaylightCaption, DaylightOffset** values are not reported.	N/A
Errors in the Notification Server computer log after an inventory policy is run on Linux computer.	When you complete running an inventory policy on Linux computer, you get multiple errors in the Notification Server computer log. The errors notify you that login session start time cannot be set.	N/A

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description	Article link
"Unsupported file filter property" error occurs in the Notification Server computer log after software inventory is collected on UNIX, Linux, and Mac computers.	You can collect software inventory using the filescan rules with the acceptable date format for **LastModifiedDate** such as YYYY-MM-DD HH:MM:SS or YYYY-MM-DD. However, after software inventory is collected on UNIX, Linux, and Mac computers, you get the error "Unsupported file filter property: "LastModified". The filter will be ignored". As a result, the data for last modified date is not collected. To work around the problem, you can create a custom inventory task to collect the data for last modified date.	N/A
Some inventory scans may take a long time to complete.	The default inventory task includes several software rules for scanning that can take quite a long time depending on the platform. For example, on Solaris platforms, the **/opt** or **/Volumes** on Mac OS directories contain multiple subfolders and files. On less powerful computers, this can take more than one hour. To avoid this, you can exclude such rules and exactly define the directories that you want to scan.	N/A
Inventory scan does not scan deeper than system limitations.	Each operating system has a maximum length paths limitation (though not the file system). For example, for Solaris and Mac OS X, by default the limit is 1024 chars, and for Linux OS, it is 4096. As a result, an Inventory scan does not detect files allocated deeper than the system limitations.	N/A
The **Manufacturer** field of the **Storage** data class may be empty.	On UNIX/Linux/Mac OS clients that have IDE disks, the **Manufacturer** field of the **Storage** data class may be empty.	N/A
Some fields of the **HW Chassis** data class may be empty on Mac OS X platform.	The fields may be empty for the following reasons: ■ Information for the fields **PartNumber** and **AudibleAlarm** is not available on Mac OS X platform. ■ The availability of the fields **PartNumber** and **SecurityBreach** depends on the current model.	N/A

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description	Article link
HW_DiskPartition data class cannot be populated on AIX platforms.	On AIX platforms, the logical volume manager (LVM) is used by default, and the current inventory data model is not capable of representing it. The Partition and Volume concept of AIX does not directly match with the fields of the **HW_DiskPartition** data class.	N/A
Not all inventory data is reported correctly on AIX platforms.	The inventory for the following data class fields is not correctly collected: **Platform | Data class | Field** AIX | **DB_DatabaseStorageArea** | **FileSystemType** for Oracle AIX | **DB_Database** | **Vendor** for MySQL AIX | **HW_PhysicalMemory** | **DataWidth** and **TotalWidth** AIX | **HW_PhysicalMemory** | **Speed** AIX | **HW_PhysicalMemoryArray** | **MaxCapacity** AIX | **HW_Chassis** | **AudibleAlarm, LockPresent, PartNumber, SecurityBreach, SecurityStatus** AIX | **HW_Chassis** | **ChassisPackageType** AIX | **OS_OperatingSystem** | **MaxProcessMemorySize** AIX | **HW_USBDevice** | all fields AIX | **HW_DesktopMonitor** | **Manufacturer, Model, MonitorType, SerialNumber, ManufacturingDate, FeatureSupport** AIX | **SW_BIOSElement** | some firmware fields AIX | **HW_DisplayController** | **MaxMemorySupported, AdapterRAM, MaxRefreshRate** AIX | **HW_Printer** | **DefaultPaperType, HorizontalResolution, VerticalResolution** AIX | **OS_OperatingSystem** | **CountryCode, NumberOfLicensedUsers, RegisteredUser, SerialNumber** As a workaround, you can run custom inventory to collect required data on AIX platforms.	N/A

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description	Article link
Not all inventory data is reported correctly on HP-UX and HP-UX IA64 platforms.	The inventory for the following data class fields is not correctly collected: **Platform | Data class | Field** HP-UX | **HW_Baseboard** | some fields HP-UX | **HW_Chassis** | **Manufacturer, AudibleAlarm, LockPresent, PartNumber, SecurityBreach, SecurityStatus** HP-UX | **HW_Chassis** | **ChassisPackageType** HP-UX | **HW_USBDevice** | **USBVersion, SerialNumber, DeviceSpeed** HP-UX | **HW_PhysicalMemory** | **Manufacturer, Speed, DataWidth and TotalWidth** HP-UX | **HW_DesktopMonitor** | **MonitorType, VideoInputMode, ManufacturingDate, FeatureSupport** HP-UX | **HW_SCSIController** | **Index** HP-UX | **SW_BIOSElement** | some firmware fields HP-UX | **HW_DisplayController** | **MaxMemorySupported, AdapterRAM, MaxRefreshRate** HP-UX | **HW_Printer** | **DefaultPaperType, HorizontalResolution, VerticalResolution** HP-UX | **OS_OperatingSystem** | **CountryCode, NumberOfLicensedUsers, RegisteredUser, SerialNumber** HP-UX IA64 | **HW_SCSIController** | **MaxTransferRate, MaxDataWidth** As a workaround, you can run custom inventory to collect required data on HP-UX and HP-UX IA64 platforms.	N/A

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description	Article link
Not all inventory data is reported correctly on Linux, Mac, and UNIX platforms.	The inventory for the following data class fields is not correctly collected: **Platform | Data class | Field** RHEL3 | **HW_DesktopMonitor** | all fields for Linux with kernel 2.4 Linux | **HW_Keyboard-Linux** | **Manufacturer** Linux | **HW_PhysicalMemory** | **Model, Manufacturer** Linux | **HW_DesktopMonitor** | **VideoInputMode, SerialNumber, ManufacturingDate, FeatureSupport** Mac | **HW_PointingDevice** | **Type** Mac | **OS_OperatingSystem** | **OSArchitecture, InstallDate, RegisteredUser** Linux, Mac | **HW_Chassis** | **AudibleAlarm, PartNumber, Model** Linux, Mac | **HW_SCSIController** | **Index, MaxDataWidth, MaxTransferRate** Linux, Mac | **HW_DisplayController** | **MaxRefreshRate, VideoProcessor** Linux, Mac | **OS_OperatingSystem** | **CountryCode, NumberOfLicensedUsers, RegisteredUser, SerialNumber** Linux, Mac, UNIX | **HW_DesktopMonitor** | **MonitorType** As a workaround, you can run custom inventory to collect required data on Linux, Mac and UNIX platforms.	N/A

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description	Article link
Not all inventory data is reported correctly on Solaris platforms.	The inventory for the following data class fields is not correctly collected: **Platform | Data class | Field** Solaris | **OS_OperatingSystem** | **CountryCode, NumberOfLicensedUsers, RegisteredUser, SerialNumber** Solaris | **HW_DisplayController** | **MaxRefreshRate, VideoProcessor** Solaris | **HW_DiskPartition** | **Bootable** Solaris | **SW_BIOSElement** | **BuildNumber, IdentificationCode, Name** Solaris | **HW_DisplayController** | **MaxMemorySupported, VideoProcessor, AdapterRAM** Solaris | **HW_Battery, HW_USBDevice** | all fields Solaris | **HW_SCSIController** | **HardwareVersion, Index, MaxDataWidth, MaxTransferRate** Solaris | **HW_SCSIController** | **HardwareVersion** for **SCSI Fibre Channel Controller** Solaris | **OS_OperatingSystem** | **MaxProcessMemorySize** Solaris x86 | **HW_Chassis** | **Model, AudibleAlarm, PartNumber, SecurityBreach** Solaris SPARC | **HW_PhysicalMemory** | all fields As a workaround, you can run custom inventory to collect required data on Solaris platforms.	N/A

Table 3-6 Known issues for Inventory Pack for Servers

Issue	Description	Article link
Server inventory policies report the incorrect database size for Microsoft SQL Server 2000.	You can gather the information about database size for Microsoft SQL Server 2000 with the **Full Server Inventory** and **Delta Server Inventory** policies. However, the policies report the database size as the size of the `.mdf` files (database files) only and do not include `.ldf` files (log files). For Microsoft SQL Server 2005 and Microsoft SQL Server 2008, the policies correctly report the sum of the `.mdf` and `.ldf` file sizes as the database size. The database size is presented in round numbers. For example, 2.4 MB are reported as 2 MB, and 2.7 MB are reported as 3 MB.	N/A
Full inventory for Microsoft SQL Server 2012 is not gathered when you run an inventory policy or task using the advanced option **System account**.	To gather full inventory for Microsoft SQL Server 2012 with the predefined policy or a custom inventory policy or task, you need to select the advanced option **Logged in user** on an inventory policy or task page, at **Advanced Options > Run Options**. If you run an inventory policy or task using the advanced option **System account**, the data is not gathered for all server inventory data classes and not all the database users are reported.	N/A
A license is not reclaimed when the **Asset Status** is set to a custom asset status.	A license is not reclaimed when the **Asset Status** is set to a custom asset status. Inventory Pack for Servers license should be reclaimed on setting the **Asset Status** other than **Active**.	N/A
An inventory task with the disabled MySQL data class but with valid MySQL credentials it collects MySQL data on Linux computers.	If you create an inventory task with the MySQL data class unchecked in the **Advanced** options, on the **Data Classes** tab, and then, on the **Run Options** tab, select valid MySQL credentials, the inventory task still collects MySQL data on target Linux computers. MySQL data must not be collected if no MySQL data class is checked in the inventory task.	N/A

Table 3-6 Known issues for Inventory Pack for Servers *(continued)*

Issue	Description	Article link
The Inventory policy or task that runs with the root rights when collecting the inventory on SUSE Linux Enterprise Server or on AIX is not able to log into the Oracle database.	The Inventory policy or task, if not specified otherwise, runs with the root rights by default. However, on SUSE Linux Enterprise Server and on AIX it is not possible to access Oracle applications while you are logged in as a root user. Because of that, the Inventory policy or task that runs with the root user credentials is not able to log in to the Oracle database. This problem does not occur on Red Hat Enterprise Linux, Solaris, and HP-UX Oracle servers. As a workaround, you can create an inventory policy or task that collects inventory for Oracle data classes only and runs with non-root user credentials. To do so, perform the following steps: 1 In the **Symantec Management Console**, click **Manage**. 2 ■ To create the corresponding inventory policy, click **Policies > Discovery and Inventory > Inventory**. ■ To create the corresponding inventory task, click **Jobs and Tasks**. In the left pane, navigate to the folder where you want to create an inventory task, right-click the folder, and then click **New > Task**. 3 On the inventory policy or task page, click **Advanced**. 4 On the **Advanced Options** page, on the **Data Classes** tab, expand **Server Inventory data classes > Databases**, and then check the **Oracle** data class. 5 On the **Run Options** tab, under **UNIX**, specify non-root user credentials. 6 Click **OK**. 7 Click **Save changes**.	N/A

Table 3-6 Known issues for Inventory Pack for Servers *(continued)*

Issue	Description	Article link
Traces in the log files.	On the target computer, Inventory Pack for Servers tries to inventory the data classes for various supported server components, such as Microsoft Exchange Server, Microsoft IIS Server, and so on, irrespective of whether server components are present. This does not result in slowing down the inventory process. However, some traces, like “Could not collect the inventory information for xxxx”, “Failed to collect inventory for xxxx”, “Execution of query Failed”, or “Failed to inventory information from WMI. Error: … ” are added to the log files when you run an inventory task for gathering server data classes with the **Enable verbose client logging** option selected at **Advanced option > Run Options**.	N/A
The **DHCP Scopes** and **DHCP Options** data classes incorrectly report the values that have double quotes.	When you define the DHCP scopes and use double quotes in the description (for example, **DHCP Scope Configuration for “Altiris” company**), the **Description** column of the **DHCP Scopes** data class reports a value only up to the first double quotes. In the given example it returns only **DHCP Scope Configuration for**. This limitation also applies to the **Scope Id** and the **Super Scope** columns of the **DHCP Scopes** data class and the **Scope Id** column of the **DHCP Options** data class. The same limitation also applies to the `netsh exec filename` command provided by the DHCP server. This command is used to import the DHCP configuration details from the text files.	N/A
The reported version of the DHCP server does not match with the DHCP version given in the **About** dialog of the DHCP server.	The **Version** column of the DHCP data class reports the DHCP version that is different from the version given in the **About** dialog of the DHCP server.	N/A

Table 3-6 Known issues for Inventory Pack for Servers *(continued)*

Issue	Description	Article link
To gather the IIS 7.0 inventory, you need to install the Management Compatibility features.	The IIS inventory that is gathered for the **IIS Application Pools** data class automatically starts the IIS Admin service if it is in a stopped state. The **Application Server Console Installed** and **Remote Admin Installed** fields from the **IIS Setting** data class are not reported on Windows Server 2008 for IIS 7.0. The Inventory Plug-in gathers the IIS inventory using IIS metabase. IIS metabase is fully supported until IIS version 6.0. With IIS version 7.0, on Microsoft Windows Server 2008, IIS metabase has been replaced by XML configuration files. To gather the IIS 7.0 inventory, you need to install the Management Compatibility features by using “Server Manager” on Microsoft Windows Server 2008.	N/A

Table 3-6 Known issues for Inventory Pack for Servers *(continued)*

Issue	Description	Article link
IIS Inventory data classes are reported incorrectly.	With IIS 7.0 installed on Microsoft Windows Server 2008, some fields of the following IIS data classes are not populated correctly, even if the Management Compatibility features are installed. Fields of **IIS Http VirtualDir Setting Data** data class: ■ Content Location ■ Default Document Enabled ■ Default Document Name ■ Script Source Access Enabled ■ Access Read Enabled ■ Access Write Enabled ■ Directory Browsing Enabled ■ SSL Access Enabled ■ Content Expiration Enabled ■ Content Expiration Setting ■ Log Enabled ■ Execute Permission Fields of **IIS Http Host Setting Data** data class: ■ Content Location ■ Default Document Enabled ■ Default Document Name ■ Script Source Access Enabled ■ Access Read Enabled ■ Access Write Enabled ■ Directory Browsing Enabled ■ SSL Access Enabled ■ Content Expiration Enabled ■ Content Expiration Setting ■ Log Enabled ■ Execute Permission Fields of **IIS Http Server Setting Data** data class: ■ Central Binary Logging Enabled ■ Rapid Fail Protection Interval ■ Rapid Fail Protection Max Crashes	N/A

Table 3-6 Known issues for Inventory Pack for Servers *(continued)*

Issue	Description	Article link
Prerequisite for gathering the inventory of **Exchange Mailboxes** data class.	On a freshly installed operating system, before executing a server inventory stand-alone package or a server inventory task for gathering Microsoft Exchange Server data classes, you must explicitly install the Microsoft Visual C++ 2005 SP1 Redistributable Package (x86). Otherwise, the inventory for the data class **Exchange Mailboxes** is not gathered. The Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) installs run-time components of Visual C++ Libraries that are required to run the applications that use these run-time components. Server Inventory Plug-in depends upon these libraries and run-time components. You can download the package for free at http://www.microsoft.com/downloads/details.aspx?familyid=200b2fd9-ae1a-4a14-984d-389c36f85647&displaylang=en	N/A
Exchange Server Inventory.	On Windows Server 2003 operating system, inventory of the **Exchange Mailboxes** data class is only populated when you use “Logged In” user context. On Windows 2000 Server Operating System, inventory of the **Exchange Mailboxes** data class is not populated. Inventory for Microsoft Exchange Server 2007 is not supported. Exchange Inventory does not return data from Exchange Server Clusters.	TECH47438
SQL Server Inventory.	The **License Type** and **Number of License** fields are not populated in the **SQL Server License** data class. If multiple instances of SQL Server are installed on the target computer, the **Inv Srv SQL Database Service** data class reports the service name without including the prefix “MSSQL$”. Inventory reports incorrect SQL instance name if a user changes the name of target computer after installing Microsoft SQL Server on it. In this case the previous name of the computer is reported as an SQL instance name in the SQL Server data classes.	N/A

Table 3-6 Known issues for Inventory Pack for Servers *(continued)*

Issue	Description	Article link
Collecting inventory using Oracle database.	Inventory Pack for Servers Plug-in for Windows does not implement the logic for populating the following fields: ■ The **Block Size** field of the **Oracle Database** data class. ■ The **Block Size** and **File System Size** fields of the **Database Storage Area** data class for Oracle 9i. ■ The **Users High Watermark** field of the **Oracle Database Service** data class. On Microsoft Windows Server 2008, the following data classes are not reported, or if reported, do not contain the inventory for Oracle: ■ **Oracle Database Service** ■ **Database System** ■ **Database Service** ■ **Associate Database System to Service**	N/A
Collecting inventory using MySQL database.	MySQL details for the **DB_Database Service** data class are not populated when MySQL service is stopped. Inventory of installations of multiple instances of MySQL Server on a computer is not supported. If multiple instances are installed, the inventory is gathered for the first instance that is found.	N/A
Collecting database inventory.	If you select any kind of database inventory (for example, Oracle, MySQL or MS SQL) from the data class tree view, Inventory gathers data for almost all the databases (Oracle, MySQL, and MS SQL) installed, irrespective of selection in the tree view because most of the data classes are common among them. If you disconnect from the registered server running SQL Server through SQL Server Enterprise Manager by right-clicking the server name and clicking the **Disconnect** menu, then after gathering the inventory, the **Operational Status** property of the **Database Service** data class is not reported.	N/A
Running an inventory task in the **Specified User** context fails.	As a workaround, please execute the inventory task in the **System** user context or in a **Logged In** user context.	N/A

Table 3-6 Known issues for Inventory Pack for Servers *(continued)*

Issue	Description	Article link
Collecting inventory on Apache web server.	Only a single instance of Apache Server is supported. Server Inventory Plug-in does not implement the logic for populating the **Host State** field of the **Http Host** data class for Apache Servers. This field is not populated in any scenarios with Apache Server. If you tag some modules that are compiled statically, the properties under such a section are retrieved and displayed without checking the specific module condition. (Windows only) If the value for the **KeepAliveTimeout** parameter is specified in the configuration file `httpd.conf` of Apache web server, then after gathering the inventory, NSE loading fails for the data class **Http Host Setting Data** on Notification Server.	N/A
Hardware inventory on Windows Server 2003 R2 SP2 (x86) computers reports incorrect processor count.	When you collect hardware inventory from Windows Server 2003 R2 SP2 (x86) computers, the number of physical processors is reported incorrectly. This happens when the client computer uses either hyperthreading-enabled processors or multicore processors because Windows Server 2003 cannot detect them. For more information on this issue and a hot fix, please see the following links: http://support.microsoft.com/kb/936235 http://support.microsoft.com/kb/932370	N/A

Fixed issues

The following are the fixed issues for this release:

Table 3-7 Fixed issues

Issue	Description	Article link
Impossible to meter Visio Professional 2010.	You cannot meter Visio Professional 2010 because it does not have any executable files that are associated with it. This fix corrects an issue with Microsoft Office Visio 2010 and other Microsoft applications.	N/A

Other things to know

The following are the other things to know about this release.

Table 3-8 Other things to know

Issue	Description	Article link
Deprecated web browser	Inventory Solution 7.5 SP1 release does not support the following web browser: ■ Internet Explorer 7	N/A
Antivirus data class has been deprecated.	**Antivirus** data class selection check box is removed from the list of Inventory data classes for the inventory policies and tasks. The inventory scan no longer reports the **Antivirus**. To gather the required information about antivirus software, you can use the Antivirus Inventory that comes with Symantec Endpoint Protection Integration Component.	N/A
SQL Server inventory in Specified User or Logged-in User context.	Inventory Pack for Servers gathers inventory for SQL Server using the **Windows Authentication** method. When using the Specified User or Logged-in User context to gather inventory for SQL Server, the user must have access rights to connect to SQL Server, otherwise the inventory for SQL Server will not be gathered.	N/A
Disabled **Auto Growth** causes blank reports for some data classes.	**Data File Growth Mode** and **Data File Growth Size** fields from **MS SQL Server Databases** data class for a database will return blank whenever **Auto Growth** property for that database is disabled.	N/A

Table 3-8 Other things to know *(continued)*

Issue	Description	Article link

Accepted MySQL connection parameters for Inventory tasks.	To access the **MySQL Credentials** dialog box, perform the following steps in order:
	■ Open an inventory task.
	■ In the right pane, click **Advanced**.
	■ In the **Advanced Options** dialog box, on the **Run Options** tab, under **MySQL**, click the **Add** symbol.
	You must specify the user name and password to connect to the MySQL Server and collect the inventory data. Specify the other connection parameters only when they differ from the default values.
	On Windows, you can specify the following connection parameters:
	■ `--host=host:port`
	Default port is 3306
	On UNIX and Linux, you can specify the following connection parameters:
	■ `--protocol={TCP|SOCKET}`
	Default protocol is SOCKET
	■ `--port=port_num`
	Default port is 3306
	■ `--socket=path`
	Default socket file is `/tmp/mysql.sock`
	You can use the following examples:
	■ To specify TCP/IP connection with port 13306:
	`--protocol=TCP --port=13306`
	■ To specify UNIX socket file `/var/lib/mysql/mysql.sock`:
	`--protocol=SOCKET`
	`--socket=/var/lib/mysql/mysql.sock`
	For more information about connecting to the MySQL Server, please refer to the following URL:
	http://dev.mysql.com/doc/refman/5.0/en/connecting.html
		N/A

Table 3-8 Other things to know *(continued)*

Issue	Description	Article link
Collecting inventory using Oracle Database (Windows only).	For gathering Oracle Database Inventory, inventory component establishes connection with the database. The user credentials provided to connect to the Oracle database must have SYS DBA privileges to gather the Oracle inventory successfully. If multiple instances of Oracle are installed, and user wants to gather inventory from that computer, then each database instance entry should be present in all `tnsnames.ora` files. That means that all the `tnsnames.ora` files related to each Oracle instance should be identical. For that to happen, a user should replicate the database entries from one `tnsnames.ora` to another. The location for `tnsnames.ora` file is `OracleHome\Network\Admin`.	N/A

Chapter 4

Inventory for Network Devices

This chapter includes the following topics:

- Known issues
- Fixed issues
- Other things to know

Known issues

The following are the known issues for this release.

Table 4-1 Known issues

Issue	Description	Article link
Separate licenses for Inventory for Network Devices are displayed in the Symantec Management Console.	Inventory for Network Devices should share licenses with Inventory Solution. Currently the licenses for these two products are separately listed in the Symantec Management Console. However, the licenses are shared, and Inventory Solution license is consumed for every device that is inventoried by Inventory for Network Devices.	N/A

Fixed issues

The following are the fixed issues for this release.

Table 4-2 Fixed issues

Issue	Description	Article link
The reports in the **Agentless Inventory** folder belong to Network Discovery.	The folder has been renamed. The Network Discovery reports are now located at **Symantec Management Console > Reports > All reports > Discovery and Inventory > Discovery**.	N/A

Other things to know

The following are the things to know about this release:

Table 4-3 Other things to know

Issue	Description	Article link
Hierarchy and replication support.	All discovered agentless inventory resources (computers, routers, switches, etc.) replicate up to the parent Notification Server. Predefined SNMP data mapping tables replicate down from the parent Notification Server to the child Notification Servers. Possible workaround: To manually replicate a custom SNMP data mapping table down from the parent Notification Server to child Notification Servers do the following: ■ In the Symantec Management Console, on the **Settings** menu, click **All Settings**. ■ In the left pane, expand **Notification Server > Resource and Data Class Settings > Data Classes > Network Resource Data**. ■ In the left pane, under **Network Device Data**, right-click the custom SNMP data mapping table that you want to replicate, and then click **Hierarchy > Replicate Now**. ■ In the confirmation dialog box, click **OK**.	N/A

Table 4-3 Other things to know *(continued)*

Issue	Description	Article link
Security and permissions.	The Symantec Management Platform provides role-based security. The Administrator role has all rights to perform all agentless inventory tasks. For other users, you can assign rights to different roles. The following are the unique privileges for Inventory for Network Devices: ■ Read SNMP Table. Lets you access the SNMP Table Mappings page for initial viewing. ■ Import SNMP Table XML. Lets you import SNMP Table mapping definitions as .XML. ■ Manage SNMP Tables. Lets you create, delete, and edit existing SNMP user tables. **Note:** Predefined tables cannot be edited. ■ Test SNMP Table Mappings. Lets you use the test SNMP functionality on the SNMP Table Mappings page.	N/A

Chapter 5

Monitor Solution for Servers

This chapter includes the following topics:

- What's new in this release
- Known issues
- Other things to know

What's new in this release

In Monitor Solution for Servers 7.5 SP1, the following new features are introduced:

Table 5-1 List of new features in Monitor Solution

Feature	Description
New **Alert resource target** filter was added to the Event Console.	New **Alert resource target** filter lets you filter the target resource by organizational group.
Remote Monitor Service (RMS) is now supported for site servers with Windows Server 2012.	Remote Monitor Service (RMS) can now be installed on site servers with Windows Server 2012 and Windows Server 2012 R2.

Known issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- Monitor Solution
  See Table 5-2 on page 69.
- Event Console
  See Table 5-3 on page 73.

Table 5-2 Known issues for Monitor Solution

Issue	Description	Article Link
A client computer operating in Cloud-enabled Management (CEM) mode is available for **Reset Monitored Resource** task run.	In some cases, monitored resource that is managed in CEM mode is available as a target for **Reset Monitored Resource** task. This situation appears if you run the task using **Quick Run** or **New Schedule** run options.	N/A
Details of forwarded alerts are not displayed correctly on the Management Station console.	After you add and save a new rule, and then send alerts based on the rule, the categories Hostname, Definition, and Protocol are not displayed correctly on the Management Station console.	N/A
Customized **Monitor Plug-in rollout** policy targets are rewritten with default values during upgrade.	When you upgrade to Monitor Solution 7.5 SP1, all customized targets for the **Monitor Plug-in rollout** policy are rewritten with default values.	N/A
Incorrect heartbeat alert behavior on a virtual machine.	A heartbeat alert may be raised in Event Console from a monitored resource that runs on a virtual machine, even if it is online and the metric provider is running.	N/A
Monitor token values that include double quotes cause **VBScript** tasks to fail.	If you have a **VBScript** client-side task that is associated with a rule and the output from a token produces double quotes, the **VBScript** fails.	TECH154599
The **Disk Paging Activity** report displays incomplete data.	The **Disk Paging Activity** report displays incomplete HP-UX and AIX data when it is viewed in the Chart View.	N/A

Table 5-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
Agentless monitoring uses Pluggable Protocol Architecture (PPA) connection profiles.	The Remote Monitoring Server (RMS) agent leverages PPA to make connections to monitored remote resources to obtain metric data. PPA references the connection profiles used during Network Discovery. The Network Discovery connection profiles define which protocols are enabled and any applicable credentials and settings for each protocol. When the RMS agent attempts to monitor an agentless resource, it queries the database and uses the connection profile that was used during Network Discovery. If the RMS agent cannot find a reference to a connection profile, the Default connection profile is used. To select a different connection profile, run a new Network Discovery and select the desired connection profile for remote resources.	N/A
Unable to assign a connection profile to a resource.	On the **Manage Connection Profile** page, when you create connection profiles for different configured clients, the user is not able to assign (to map) connection profiles to the resources.	N/A
WS-Management service cannot process the request on Windows clients.	WS-Management service does not work on Windows clients because it cannot process the request. The service cannot find the resource that the resource URL and selector identify.	N/A
Time drifting issues occur when monitoring heartbeats on Linux computers that are hosted on VMware.	When monitoring heartbeats on Linux computers that are hosted on VMware, there are issues with time drifting. This issue can cause Notification Server to receive heartbeats with a very long delay and an alert to be raised in the Event Console. To avoid issues with unnecessary alerts in the Event Console, make sure that your heartbeat time settings are synchronized to account for possible time drifting.	N/A
The Poll Metric on Demand task cannot poll agent-based metrics on a computer that does not have the Monitor Plug-in.	The **Poll metric on demand** task can poll two different types of metrics: agent-based and agentless. It is supported on two different types of targets: with and without Monitor Plug-in. If the **Poll metric on demand** Task is executed on an agentless target without the Monitor Plug-in installed, then it can only poll agentless metrics on that computer. Agent-based metrics are not polled on an agentless client computer as agent-based metrics require the Monitor Plug-in to run.	N/A

Table 5-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
Network Discovery found devices may not be listed in the targeted filters of the default agentless policy.	Agentless monitor policies target filters of computers and devices. By default, the target includes only unmanaged devices running Windows Server 2003, Windows Server 2008, or Windows Server 2012. When computers are discovered, the local operating system is a property of that computer resource. If during discovery, a computer's operating system cannot be determined, an operating system-specific filter does not recognize that computer. If an agentless monitor policy is not running on a computer as expected this issue is a possible cause. **Note:** The operating system version is correctly discovered for the target computers that have SNMP enabled.	N/A
A failed heartbeat may not raise an alert if the **Check for heartbeat every** option is less than the **Send heartbeat every** option with zero retry attempts.	A failed heartbeat may not raise an alert in the Event Console due to network latency when you have the following configuration: ■ The **Retry every** option on the **Heartbeat** tab of the **Monitor Server Settings** page has a value of "0". ■ The value of the **Check for heartbeats every** option is less than or equal to the **Send heartbeat every** option on the **Data Collection** tab of the **Monitor Plug-in Configuration Settings** page. In this case, a Monitor Plug-in may appear to occasionally go down only to come right back up again. However, the uptime data is not affected in this case.	N/A
Agentless monitoring is not available for the targets that have been discovered through an Active Directory Import.	You cannot apply agentless monitor policies to targets that have been discovered through an Active Directory Import. Workaround: Use a Network Discovery or a WINS import instead of an Active Directory Import.	N/A
You must reconnect the Real-time Performance Viewer if metric data becomes unavailable.	When you use the Real-time Performance Viewer, if a metric becomes unavailable and then becomes available again, updated data is not displayed. The viewer continues to display the data value that was last received before the metric became unavailable. The Real-time Performance Viewer must be re-connected to the target computer before updated data is reflected in the viewer.	N/A
There is a delay in the Computers List for the Real-time Viewer and Historical Performance Viewer.	Computers are not populated in the Computers List for the Real-time Viewer and Historical Performance Viewer until data is received from the target computer by Notification Server.	N/A

Table 5-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
When **Altiris** log type is selected, the Log Event metric only supports Windows platforms.	When the **Altiris** log type is selected, the Log Event metric uses Notification Server log file as source. This type of log is supported for Windows platforms only.	N/A
HTTP metrics do not support virtual hosts.	The HTTP metric cannot be used with virtual hosting. The HTTP metric only supports the use of the current host name of a physical computer that reports basic inventory to the Notification Server computer.	N/A
WMI metrics read the data with the lowest polling interval.	If two WMI metrics are configured to parse the same command output and they both have different polling intervals, these metrics read the data with the lowest polling interval. The WMI metrics combine into a similar query for optimization. The query runs at the lowest interval setting.	N/A
Polling metric on-demand task fails.	If you add the **Poll metric on demand** task to a policy or to a rule, then the task fails to run when the rule is activated. The task completes successfully when manually executed.	N/A
Manually created Monitor site servers disappear after disaster recovery.	Monitor site servers that are created manually disappear after disaster recovery. Workaround: Create Monitor site servers again, manually.	N/A
SQL metric default connection data must be provided to configure **All Windows Servers** policy.	It is possible to save the **All Windows Servers** policy configuration, without providing all information required under **SQL metric default connection**. To use SQL metrics you must provide information in all fields under **SQL metric default connection**. You do not have to provide all data, if you do not intend to use SQL metrics.	N/A
Log Event metric for FTP log file with **Unlimited file size** setting produces incorrect results.	On Windows Server 2003, Windows Server 2008, or Windows Server 2012 the **Log Event** metric for the FTP log file, with the **Unlimited file size** setting enabled, during the agent-based monitoring, triggers the rule incorrectly. When FTP log file size is set to *unlimited*, Monitor Agent functionality is unable to determine when changes are made to the log and metric data in not parsed by the Agent from the FTP log file. Workaround: Set a constant file size (for example, 64K) for the FTP log file, instead of *unlimited*, when configuring **Log Event** metric.	N/A

Table 5-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
Aggregation can only evaluate metrics if they monitor an equal number of instances.	If one of the two metrics inside the rule monitors more instances than the other one, the aggregation logic evaluation may produce unexpected results.	N/A
Policies may get overwritten, when creating multiple policies in a new window or from the Server Management Suite portal.	On the **Home** menu click **Monitoring and Alerting**. In the left pane expand **Monitor > Policies**, and then right-click the name of the policy, and click **Open in New Window**. If several policies are created in the same manner, every subsequent policy rewrites all the previous ones. When policies are turned on from the Server Resource Manager View of the Server Management Suite Portal, the same result is produced – last policy overwrites all previous ones. Workaround: To get back the overwritten policies, re-import the rewritten monitor packs manually. All monitor pack settings will also be reset to default in this case.	N/A

Table 5-3 Known issues for Event Console

Issue	Description	Article Link
It is not possible to export or import **Alert Rule Settings** from **Event Console**.	It is not possible to export and import **Alert Rule Settings** from the **Event Console** page. Workaround: On a source server, do the following: ■ In the Symantec Management Console, on the **Settings** menu, click **Monitoring and Alerting**. ■ In the left pane, expand **Event Console**, and click **Alert Rule Settings**. ■ In the right pane, right-click each rule, and then click **Export**. ■ Save the rules. On a target server, do the following: ■ In the Symantec Management Console, on the **Settings** menu, click **Monitoring and Alerting**. ■ In the left pane, expand **Event Console**, and click **Alert Rule Settings**. ■ In the right pane, right-click on any item in the list, and then click **Import**. ■ Select the previously saved rules.	N/A

Table 5-3 Known issues for Event Console *(continued)*

Issue	Description	Article Link
The **Acknowledge** and **Resolve** options become disabled in some cases.	When you select multiple alerts holding down the Shift key, the **Acknowledge** and **Resolve** options on the toolbar become unavailable. Workaround: Right-click any of the selected items and click **Acknowledge** or **Resolve**.	N/A
In the **Event Console**, the **Select Filter** text box does not support Double-byte Character Sets (DBCS) input.	In the **Event Console**, the **Select Filter** text box has a limitation. The DBCS input is not supported from neither a physical keyboard, nor using the IME virtual keyboard. Workaround: You can copy DBSC text and paste it into the **Select Filter** text box.	N/A
Internet Explorer error message **about:blank** pops up.	Internet Explorer error message **about:blank** pops up: **Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration.** Workaround: **about:blank** needs to be added into the **Trusted sites** list of the Internet Explorer.	N/A

Other things to know

The following are the things to know about this release. If additional information about an item is available, the item has a corresponding article link.

The other things to know are separated into the following groups:

- Monitor Solution
  See Table 5-4 on page 75.
- Event Console
  See Table 5-5 on page 76.

Table 5-4 Other things to know about Monitor Solution

Items	Description	Article Link
You may need to install `sysstat` on your monitored Linux computers.	You must install `sysstat` on your targeted Linux computers to use the following monitor policies: ■ Processor ■ Disk I/O ■ Memory ■ Linux Server Health	N/A
The repeat count feature specifies the number of times the rule must trigger in a row before an action is taken.	After the repeat count specified in a rule has been reached, the rule resets to "normal" on the next value, even if that value crosses the threshold. If the value crosses the threshold, the rule restarts the repeat count for the next evaluation. Example: Rule count definition - if CPU > 10 for 3 times. If the values are 11, 12, 13, 11, the rule triggers on the third value and then resets to normal on the fourth value. **Note:** Repeat count for rule increases for each condition which is met instead of for the overall criteria for the rule.	N/A
Activated Monitor Policies Web Part only shows the policies that the Monitor Plug-in has activated.	The Monitor Plug-in must first activate a monitor policy before it is displayed in the **Activated Monitor Policies** Web Part of the **Monitoring and Alerting** home page. If you enabled a monitor policy but it is not yet displayed in the Web Part, it might be because the Web Part is populated from inventory data that is received from the plug-in	N/A
Purging log event and Syslog data.	Both log event and Syslog data purging is controlled with the single String metric data purging schedule. To schedule string metric data purging: 1 In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**. 2 In the left pane, click **Monitoring and Alerting > Monitor > Settings > Monitor Server Settings**. 3 On the **Monitor Server Settings** page, click the **Purge Maintenance** tab. 4 Under **Non-numeric Data**, set the value for **String metric data**. 5 On the **Monitor Server Settings** page, click **Save changes**.	N/A

Table 5-4 Other things to know about Monitor Solution *(continued)*

Items	Description	Article Link
The specific setup is required to enable Smart Metrics using SNMP.	To enable Smart Metrics using SNMP: ■ The SNMP service must be installed on the monitored computer. ■ The community name must be configured in the SNMP service on the monitored computer. The community name must match the community string in the SNMP protocol settings for your connection profile. ■ SNMP packets must be accepted from any host in the SNMP properties on the monitored computer.	N/A
How WMI Metric handles WMI property arrays.	In some cases WMI property values are stored as arrays of values. In this case, each property in the array is represented as a different instance\value pair for the metric. The name for instance is "Name of the instance (n)" where n is the index. For example, if % disk space had multiple properties for disk space: "C: (1)" = 23, "C: (2)" = 43, "D: (1)" = 54, "D: (2)" = 7	N/A

Table 5-5 Other things to know about Event Console

Items	Description	Article Link
Help is not available on the **Workflow rule** tab.	On the **Workflow rule** tab of the **Alert Rule Settings** page, the context-sensitive Help may not appear when you click F1. To display the context-sensitive Help for the **Workflow rule** tab, you must first create a workflow rule and click on the Web Part that contains the rule before clicking F1.	N/A

Chapter 6

Patch Management Solution for Linux

This chapter includes the following topics:

- Known issues
- Fixed issues
- Other things to know

Known issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- Installation and upgrade issues
  See Table 6-1 on page 77.
- Hierarchy and replication issues
  See Table 6-2 on page 78.
- Other known issues
  See Table 6-3 on page 79.

Table 6-1 Installation and upgrade issues

Issue	Description	Article Link
Steps to do after upgrading from an earlier version.	Run the Import Patch Data for Novell and Import Patch Data for Red Hat tasks with the **Incremental Import** box unchecked.	N/A

Table 6-1 Installation and upgrade issues *(continued)*

Issue	Description	Article Link
Invalid custom severities are not removed from the bulletins.	Invalid custom severities are cleaned up during upgrade. However, bulletins keep the invalid severities assigned to them. To remove an invalid severity from a bulletin, change its severity by using the right-click menu.	N/A
SQL queries in automation policies are overwritten.	Parameters in the default automation policies can be migrated, but SQL queries are overwritten. Symantec recommends that if you want to customize an automation policy, you clone the policy, and then make changes to the clone.	N/A
Novell resources do not merge during import after the upgrade to 7.5 SP1.	After an upgrade from 7.1 SP2 to 7.5 SP1, some resources for Novell do not merge properly during the Novell import. To delete empty bulletins with old names, you need to run the import with the **Delete data for excluded software channels** box checked.	N/A

Table 6-2 Hierarchy and replication issues

Issue	Description	Article Link
Only two-level hierarchy is supported.	Although Symantec Management Platform lets you create multi-level hierarchies, Patch Management Solution supports only two-level hierarchy. A child Notification Server computer cannot be a parent to another Notification Server computer.	HOWTO44217
Scheduled client tasks are not replicated to child immediately.	When you create a schedule for a client task (for example, **Run System Assessment Scan on Linux Computers**), and include managed computers from a child into the target, the schedule does not replicate to the child Notification Server computers immediately. Workaround: Use the **Run now** option on the task page.	N/A
Exporting software update policies from parent to child is not supported.	Do not attempt to export a software update policy on the parent Notification Server computer and import it on the child. Instead use the built-in replication functionality.	N/A
An issue with **Allow Package Server Distribution with Manual Prestaging** setting.	The **Allow Package Server Distribution with Manual Prestaging** settings are replicated, but displayed incorrectly in the Symantec Management Console of the child Notification Server computer. The functionality is not affected, you can ignore this user interface issue.	N/A
Reports do not display any data from hierarchy.	With the exception of the **Compliance Summary** report, Patch Management Solution reports do not display any data from the child Notification Server computers. Only the data for the current Notification Server computer is displayed in patch reports.	N/A

Table 6-2 Hierarchy and replication issues *(continued)*

Issue	Description	Article Link
Packages are not replicated to child.	Child Notification Server computers download packages from Novell and Red Hat servers after the Patch metadata is replicated down the hierarchy.	N/A
Replicating data between different versions of Patch Management Solution is not supported.	Although some items may replicate between different versions of Patch Management Solution that are installed on parent and child Notification Server computers, Symantec does not recommend this. If you want to use hierarchy and replication, Patch Management Solution versions must be the same on the parent and child.	N/A

Table 6-3 Other known issues

Issue	Description	Article Link
Some software packages in SUSE Enterprise Linux Server/Desktop 11 SP3 are In lower version than in SP2.	Some packages that are installed on SLES/SLED SP3 client computers are in lower version than in SLES/SLED 11 SP2. This issue might cause that unwanted packages from SLES/SLED 11 SP2 channel are updated on SLES/SLED 11 SP3 client computers.	N/A
Relocating packages from an UNC location to another location does not work.	If, on the **Core Services** page, you change the **To Location** value from an UNC path to another path, the packages will not be relocated. Workaround: Relocate the packages manually.	N/A
Software updates cannot be downloaded from an alternate download location on a non-IIS package server.	Only UNC paths can be used as an alternate download location on a non-IIS Windows package server. If you specify a local path on the server as the alternate download location, the software updates are not downloaded from a package server that does not have IIS installed.	N/A
The Patch Administrator cannot edit the default targets in the patch management configuration policies.	A user who belongs to the **Patch Management Administrators** role cannot edit default targets in the following policies: ■ Novell patch management configuration policy You access this policy from **Settings > Software > Patch Management > Novell Settings > Novell**. ■ Red Hat patch management configuration policy You access this policy from **Settings > Software > Patch Management > Red Hat Settings > Red Hat**. Workaround: On the configuration policy's page, delete the default targets, and then add the appropriate custom targets.	N/A

Table 6-3 Other known issues *(continued)*

Issue	Description	Article Link
Task details do not show the cause of the **Import Patch Data for Red Hat** or the **Import Patch Data for Novell** failing due to lack of free space on the Notification Server computer.	When there is no free space on the Notification Server computer, the **Import Patch Data for Red Hat** and **Import Patch Data for Novell** fail. When you open the task details in the **Task Status** table, no mention is made of the lack of free space causing the task to fail.	N/A
The **Novell/Red Hat Compliance by Update** report can show incorrect data.	The **Novell/Red Hat Compliance by Update** report can show incorrect number of computers on which updates have been installed. For example, this happens when the same update belongs to two different channels. Such an update is displayed as if it was installed on two computers. To work around this issue, use the report's parameters section to filter the results by operating system or by software channel.	N/A
Sometimes a software update policy fails to save.	This issue may occur when anonymous access is enabled for the Altiris folder in IIS.	N/A
Automation policy report **Maintain Retired Machine Historical Data** does not return any result.	The automation policy creates a report, but it contains no data.	N/A
Steps to do if installation fails.	Sometimes bulletin can fail to install because of a conflicting bulletin included into the same software update policy. To work around this issue, Symantec recommends that you create a software update policy for this failing bulletin only. If it still fails, you can set the log level to DEVNOTE and examine the rpm output. You can also try to install the update and its dependencies manually.	N/A

Fixed issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 6-4 Fixed issues

Issue	Description	Article link
Duplicates are created if the MetaData Import task is run after software inventory is collected from Linux client computers.	Duplicates are created during the execution of the Red Hat or Suse Linux Patch Management Import task if Linux client computers have already sent in their first-time software inventory, before the MetaData Import task was run.	TECH210368
The **Delete data for excluded software channels** may fail to delete the corresponding data.	Checking the **Delete data for excluded software channels** does not delete the data that has already been downloaded for the previously selected channels.	N/A
The **Software Update Tasks Delivery Summary** Web Part shows executed tasks as incomplete.	In the **Red Hat/Novell Software Update Tasks Delivery Summary** Web Part, the tasks that were executed more than 30 days ago are shown as Incomplete.	N/A

Other things to know

The following are the things to know about this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 6-5 Other things to know

Issue	Description	Article Link
You can use the **First Time Setup** portal to configure Patch Management Solution for the first time.	If you want, you can use the wizard on the **Home > Notification Server Management > First Time Setup** page to configure Patch Management Solution for the first use. Perform the following steps in order: 1 On the portal page, under **Step 5 - Schedule Patch Management**, click **Schedule Patch**. 2 In the wizard, configure the schedules for the patch metadata import tasks. If you want to enable more than one task, make sure the schedules are staggered to prevent the server from overloading. When you turn on the Linux tasks, you must type the Novell Mirror Credentials and the Red Hat Network access credentials. By default, all vendors and all channels are enabled. You can customize the settings later on the appropriate Import Patch Data pages. 3 (Optional) Configure the notification options. If you enable administrator notifications, you must also configure the SMTP server Settings. You can configure SMTP settings on the **Settings > Notification Server > Notification Server Settings** page. 4 On the next panel, configure the assessment scan and update installation schedules or leave the default ones. 5 Click **Schedule patch**.	N/A
Updates download URLs for Novell and Red Hat.	The software updates metadata is downloaded from the following URLs: ■ Red Hat — http://xmlrpc.rhn.redhat.com ■ Novell — https://nu.novell.com Make sure that your firewall and proxy configuration allows network communication to these URLs.	N/A
Entitlement check is removed from the product.	Patch Management Solution for Linux no longer checks for entitlement. For this reason, inventory policies and the Update Agent Discovery task are removed from the product.	N/A
Use mirror credentials for Novell.	In the previous versions of Patch Management Solution for Linux, you used Novell Customer Center credentials. Starting from version 7.1, you must type the Novell Mirror credentials on the **Novell** page, **Novell Customer Center** tab.	N/A

Table 6-5 Other things to know *(continued)*

Issue	Description	Article Link
Log file is created on the endpoint.	A log file is created on the endpoint that lets you troubleshoot patch installation issues for the particular computer. The log file location is `swuagent/var/InstallLog.txt`	N/A
Integrating Patch Management Solution with IT Analytics solution.	IT Analytics solution provides reports that display patch management data. By default, users with **Patch Administrator** role do not have access to these reports. To grant access, add the **IT Analytics Users** role to the users. For more information, see the IT Analytics documentation.	N/A
Patch Management Solution for Linux creates a new Software association type during Patch data import.	This is done for binding Linux update channels with exact OS version. This is working as designed.	HOWTO65658

Chapter 7

Patch Management Solution for Mac

This chapter includes the following topics:

- Known issues
- Fixed issues
- Other things to know

Known issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 7-1 Known issues

Issue	Description	Article link
The updates that require user interaction cannot be installed.	Patch Management Solution for Mac does not support installing updates that require user interaction.	N/A
Some firmware updates for Mac computers might not be displayed automatically in Patch Management Solution for Mac.	The Mac Software Update Helper Tool might not detect some firmware updates for Mac computers. Therefore, those updates do not appear in the **Available Mac Software Updates** report. Workaround: Manually download the update from the Apple Downloads site. If you are unsure whether your computer needs a particular update, download and open the update installer. The installer indicates whether the firmware update is already installed or is not needed.	N/A

Fixed issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 7-2 Fixed issues

Issue	Description	Article link
A manual update of the IIS configuration is required after you upgrade the IT Management Suite from 7.0 to 7.1 or later.	After you perform the upgrade from 7.0 to 7.5 SP1, you must manually update the **Physical Path** value for the following node in the IIS Manager: `Default Web Site/Altiris/Packages /{3fb61de0-7af0-40b3-a40e-2f303410715d}` Set the **Physical Path** value to the actual location of the package. By default, the package location is as follows: C:\Program Files\Altiris\Patch Management\Mac\Packages\SoftwareUpdateHelper\	N/A

Other things to know

The following are the things to know about this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 7-3 Other things to know

Issue	Description	Article link
Hierarchy is not supported.	This product does not support hierarchy and replication.	N/A
Client Mac computers must have Internet access.	Client Mac computers download updates directly from the Apple website.	N/A

Table 7-3 Other things to know *(continued)*

Issue	Description	Article link
About Patch Management security roles.	You can assign the following security roles to Symantec Management Console users: ■ **Patch Management Administrators** ■ **Patch Management Rollout** Users with **Patch Management Administrators** role have full access to Patch Management Solution functionality, but no access to the rest of the Symantec Management Console. Users with **Patch Management Rollout** role have limited access to the following Patch Management Solution functionality: ■ Software Update policies ■ Reports ■ **Patch Remediation Center** page Users with **Patch Management Rollout** role can perform the following actions: ■ Enable/disable/change settings in the software update policies ■ View reports	N/A

Chapter 8

Patch Management Solution for Windows

This chapter includes the following topics:

- Known issues
- Fixed issues
- Other things to know

Known issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- Installation and upgrade issues
  See Table 8-1 on page 88.
- Hierarchy and replication issues
  See Table 8-2 on page 89.
- Software updates installation issues
  See Table 8-3 on page 90.
- Other known issues
  See Table 8-4 on page 92.

Table 8-1 Installation and upgrade issues

Issue	Description	Article link
After the upgrade, the **Assessment Scan** policy fails to run on client computers.	A Patch Management Solution for Windows upgrade issue occurs in the following scenarios: ■ IT Management Suite upgrade from 7.1 SP2 MP1 to 7.5 ■ IT Management Suite upgrade from 7.1 SP2 MP1.1 to 7.5 SP1 ■ IT Management Suite upgrade from 7.5 to 7.5 SP1 After the upgrade, the `AexPatchAssessment.exe` is removed from **{Installation Directory}\Patch Management\Packages\WindowsVulnerabilityScan**, and the **Assessment Scan** policy fails to run on client computers. To avoid this issue, you need to run the **Import Patch Data for Windows** task after you perform the upgrade.	HOWTO95567
Invalid custom severities are not removed from the bulletins.	Invalid custom severities are cleaned up during upgrade. However, bulletins keep the invalid severities assigned to them. To remove an invalid severity from a bulletin, change its severity by using the right-click menu.	N/A
An issue when breaking the hierarchy before migrating to 7.5 SP1.	You must break the hierarchy if you are performing an upgrade to 7.5 SP1. After you break the hierarchy on the parent Notification Server computer, sometimes the child Notification Server computer retains its association with the parent server. Workaround: Also break the hierarchy on the child Notification Server computer.	N/A
SQL queries in automation policies are overwritten.	The query parameters in the automation policies (**Item Status Changed After PM Import**, **Maintain Retired Machine Historical data**, **Software Update Advertisement Disabled**, **Software Update Policy Failed**) are not migrated during an upgrade from 7.x to this version of Patch Management Solution. Parameters in the default automation policies can be migrated, but SQL queries are overwritten. Symantec recommends that if you want to customize an automation policy, you clone the policy, and then make changes to the clone.	N/A
Software update packages are not migrated to 7.5 SP1 in case of an off-box upgrade.	If you are performing an off-box upgrade to 7.5 SP1 (installing on a new computer) and using migration wizard to transfer data, the software update packages are not migrated. You must copy the packages manually or use a network location to store the packages.	N/A

Table 8-1 Installation and upgrade issues *(continued)*

Issue	Description	Article link
The **Alternative Location** settings and credentials are not migrated from 7.1 SP2.	When you upgrade from 7.1 SP2 to 7.5 SP1 and run the **Import Patch Data for Windows** task, the **Alternative Location** settings and credentials are not migrated.	N/A
Windows Computers with Software Update Plug-in counter does not show the count of the agents with non-upgraded plug-ins.	When you upgrade to 7.5 SP1, the **Windows Computers with Software Update Plug-in** counter in the **Patch Configuration Summary** Web Part does not show the count of the agents with non-upgraded plug-ins. To obtain the correct data, you need to upgrade the Software Upgrade plug-in to the 7.5 SP1 version.	N/A
The legacy Software Update Plug-in cannot be uninstalled unless it is upgraded to 7.5 SP1.	You cannot uninstall the legacy Software Update Plug-in with the **Software Update Plug-in Uninstall** policy unless you upgrade Symantec Management Agent and Software Update Plug-in to the 7.5 SP1 version.	N/A

Table 8-2 Hierarchy and replication issues

Issue	Description	Article link
Only two-level hierarchy is supported.	Although Symantec Management Platform lets you create multi-level hierarchies, Patch Management Solution supports only two-level hierarchy. A child Notification Server computer cannot be a parent to another Notification Server computer.	HOWTO44217
The **Check Software Update Package Integrity Task** cannot be run on the child.	The **New schedule** button on the **Check Software Update Package Integrity Task** page is disabled on the child Notification Server computer. Workaround: Schedule the task on the parent Notification Server computer. Then edit the schedule on the child.	N/A
The **Vulnerability Scan** task fails if the patch data has not been replicated.	If you run complete replication but do not replicate the patch data, and then try to run the **Vulnerability Scan** task on a child server or a client computer from the Parent Notification Server, the scan will fail.	N/A
Replicated Policies Get Deleted on the Child Notification Server, when using **Standard Replication Schedule**.	Replicated policies get deleted on the Child Notification Server, when Patch Management Import Data for Windows uses the **Standard Replication Schedule**.	TECH210370

Table 8-3 Software updates installation issues

Issue	Description	Article link
A box that you uncheck on page 1 in the **Distribute Software Updates** wizard does not stay unchecked when you switch to the page 2.	In **Patch Remediation Center**, choose a bulletin that has more than 10 packages for distribution. When, in the **Distribute Software Updates** wizard, on page 1, you uncheck a box that is checked by default, and then move to page 2, this box does not stay unchecked. Workaround: In the Symantec Management Console, on the **Manage** menu, click **Policies**. Create a software update policy, configure, and then enable it.	N/A
Installation of some updates cannot be performed silently.	Some updates do not support silent installation. Some dialog or progress windows may be visible to the user of the managed computer. This issue does not affect the installation, and can be ignored.	N/A
Installation of some software updates may fail.	Some updates may fail to install in certain conditions. The following updates are known to have issues: ■ Flash Player All Mozilla Firefox browser windows and all instances of Flash Player must be closed before installation. Symantec recommends that you update Flash Player 7.x, 8.x, and 9.x to the latest version. ■ Real Player Installation may fail if a limited user is logged in to the system. ■ Mozilla Firefox version 1.5, 2.0 and 3.0 All Mozilla Firefox browser windows must be closed before installation. ■ Opera Silent installation may fail on Windows XP. ■ Adobe Reader version 7 and 8 All instances of Adobe Reader, including those opened inside of a browser, must be closed before installing updates. Symantec recommends that you install Adobe Reader updates shortly after a computer restart. ■ ISA Server 2000 Security Patch for Web Proxy Service and H.323 ASN DLL (MS01-045) Installation of this hot fix requires user interaction on the target computer. The user must click **Yes** in the installation dialog box. Additional information about update installation prerequisites may be available in the Resource Manager or on the vendor's website.	HOWTO54657

Table 8-3 Software updates installation issues *(continued)*

Issue	Description	Article link
Some software updates are shown as not installed in the **Windows Update** dialog box.	Some software updates that you install using Patch Management Solution can be shown as not installed on the managed computers, in the **Windows Update** dialog box. This issue occurs because the executable is a full software release, not a patch. Symantec recommends that you use Altiris Software Management Solution from Symantec to roll out this software. The following software updates are known to have this issue: ■ KB982671 - Microsoft .NET Framework 4 ■ KB968930 - Windows PowerShell 2.0 and WinRM 2.0 ■ KB940157 - Windows Search 4.0 IE8 - Internet Explorer 8 ■ KB2526954 - Microsoft Silverlight IE9 - Internet Explorer 9 ■ KB2463332 - Windows Internal Database Service Pack 4	N/A
Some updates require original installation media.	Some updates may require original installation media. The updates that are known to require one are as follows: ■ Microsoft Project 2003 SP3 ■ Microsoft Visio 2003 SP3 ■ Citrix Presentation Server If the product was installed from a CD/DVD, then the original CD/DVD must be inserted in the disk reader on the client computer. If the product was installed from a network location, then anonymous access from the client computer to this location must be available to install the update	N/A
Microsoft Office components must be on the same Service Pack level.	Issues occur when various Microsoft Office components are having different Service Pack versions applied.	N/A
A removed vendor or software update is displayed in the **Vendors and Software** list.	If a vendor or software release is removed from Patch Data, this vendor or software release is still displayed under **Vendors and Software** list on the **Import Patch Data for Windows** page after the **Vendors and Software** list is updated. The removed vendor or software release will disappear from the list after the **Import Patch Data for Windows** task is completed.	N/A

Table 8-3 Software updates installation issues *(continued)*

Issue	Description	Article link
The **Windows Computers with Software Update Plug-in** counter works only for the client computers that have the Software Update plug-in originally rolled out from the same Notification Server.	The counter excludes the client computers' clients that were redirected from another Notification Server after the Software Update plug-in rollout. It will include the redirected client computers only after they are reinstalled or upgraded.	N/A
If you change the package location from default to **Alternative Location** with custom credentials and then back to default, you will not be able to perform **Vendors and Software** update.	When, on the **Import Patch Data for Windows** page, you change the package location from default to **Alternative Location** with custom credentials and then back to default, you will not be able to perform **Vendors and Software** update. To complete the update, you need to select **Default Location** and complete the **Vendors and Software** update. You can then switch back to the **Alternative Location**.	N/A
When you deploy Microsoft updates through Patch Management with the restart settings disabled, the operating system still forces the client computers to restart.	To turn off the Windows Updates, on the client computer, you need to enable the **Never check for updates (not recommended)** option. **Warning:** Do not disable Windows Update service because it is required for successful patching via .MSU files.	N/A

Table 8-4 Other known issues

Issue	Description	Article link
An issue when using FTP as patch data alternative download location.	If you want to use an FTP location as the alternative download location on the **Import Patch Data** page, on the Notification Server computer, add the `C:\Program Files\Altiris\Notification Server\Bin\AeXsvc.exe` service to the firewall Exception List.	N/A
An issue occurs when accessing the `AexPatchUtil.exe` utility.	A non-administrator cannot navigate to the AexPatchUtil.exe utility using the command prompt because of access restrictions to the `C:\Program Files\Altiris` folder. This issue occurs only on the Notification Server computer. Workaround: `cd` straight to the `C:\Program Files\Altiris\Altiris Agent\Agents` directory.	N/A

Table 8-4 Other known issues *(continued)*

Issue	Description	Article link
An issue with re-imaged endpoints.	An issue occurs when you re-image or reinstall an operating system on an endpoint. Software update plug-in is not able to process the policies and install software updates. Workaround: Restart the Symantec Management Agent service or restart the computer.	N/A
Patching of software that is installed into a virtual layer is not supported.	Patches that you apply to the software in a virtual layer might not be applied correctly and can corrupt the system.	N/A
Packages are not always downloaded to managed computers at the correct time.	Occasionally, software update packages may not be downloaded immediately to managed computers. This is due to a timing issue where the initial download is not triggered by Software Management and the status of the package is not updated. The packages will be downloaded when the update install schedule fires or when the next maintenance window opens.	N/A
When you click **Save Changes** in a policy, a confirmation message displays "Saved Changes" even though the policy is still being saved.	When you edit a Software Update policy, the screen is updated with the text "Saved Changes" even though the task that saves the changes made to the policy and underlying advertisements may still be running. If the changes that you made do not appear on the screen immediately, refresh the screen after a few seconds. Your changes should appear after the refresh.	N/A
The Software Update Plug-in stays in the "Update Pending" state after the dialog box closes.	Occasionally, clicking **Install Now** on the **Software Update Installation** dialog box or waiting for the dialog box to close itself does not result in the immediate installation of a software update. The installation starts five minutes after the dialog box has closed, when the Software Update Plug-in wakes up and checks its state.	N/A
The **Software Bulletin Details** report shows the computers that are out of the scope of the current console user.	In the **Software Bulletin Details** report, in the **Applies To** column, the number of all applicable computers is shown, including those for which the current console user has access and those for which access is disabled.	N/A
Update installations that require a computer restart are shown as complete.	The **Windows Software Update Delivery Summary** report shows update installations that require computer restart as complete. You can use the **Restart Status** report to view if any computers are pending restart.	N/A

Table 8-4 Other known issues *(continued)*

Issue	Description	Article link
The client computers are sometimes listed in the **Windows Computers Not Reporting System Assessment Scan Data** report, even though the **Vulnerability Scan** was successful.	The client computers are sometimes listed in the **Windows Computers Not Reporting System Assessment Scan Data** report, even when the **Vulnerability Scan** is executed successfully on them. This happens if the software releases that are installed on these computers are not selected in the **Windows Patch Data Import Task**.	N/A
The modified update will not be re-downloaded when the **Revise** option is enabled.	If you change the settings of the **Advertisement Set** policy, and then run the Patch Management with the **Revise** option enabled, the modified update will not be re-downloaded.	N/A
The out-of-scope client computers are displayed in the **Compliance Summary** report.	The **Compliance Summary** report displays the summary for the total number of Notification Server client computers, including the out-of-scope client computers. The drill-down report displays detailed information for the computers from the trusted scope only.	N/A
if you enter the **Alternative Location** path in the wrong format, the new location will still be saved successfully, but, the import will fail.	When, on the **Import Patch Data for Windows** page, under **Package Location**, you select **Alternative Location**, you need to enter it in the following format, as follows: **<alternative location>/pmimport.cab** Otherwise, if you enter the path in the wrong format, the new location will still be saved successfully, but, the import will fail.	N/A
After the disaster recovery, you need to rerun the Patch Management import.	After you have performed the disaster recovery, you need to rerun the Patch Management import.	N/A
Only UNC paths can be used as an alternate download location on a non-IIS Windows package server.	Only UNC paths can be used as an alternate download location on a non-IIS Windows package server. If you specify a local path on the server as the alternate download location, the software updates are not downloaded from a package server that does not have IIS installed.	N/A

Fixed issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 8-5 Fixed issues

Issue	Description	Article link
An issue occurs when installing Sun-Java updates.	When Java software is in use on the client computer, the update cannot be installed silently. A "Close applications" dialog box appears on the client that prevents the update process from proceeding.	N/A
Sun-Java gets uninstalled if Internet Explorer is open at the time of installation.	If an Internet Explorer window is open on an endpoint at the time of Sun-Java update installation, Sun-Java gets completely uninstalled from the endpoint. The uninstall is performed silently and the status of software update installation is **Installed**. JAVA6-27 and JAVA6-29 are among the bulletins that are known to have this problem.	N/A
Moving or deleting a folder or a file takes too much time.	If, after you generate Patch data (at least 10000 packages), you move or delete a folder or a file, it takes about 3 minutes until the action is completed. This problem is connected with the performance of Windows Shell.	N/A

Other things to know

The following are the things to know about this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 8-6 Other things to know

Issue	Description	Article link
You can use the First Time Setup portal to configure Patch Management Solution for the first time.	If you want, you can use the wizard on the **Home > Notification Server Management > First Time Setup** page to configure Patch Management Solution for the first use. Perform the following steps in order: 1 On the portal page, under **Step 5 - Schedule Patch Management**, click **Schedule Patch**. 2 In the wizard, configure the schedules for the patch metadata import tasks. If you want to enable more than one task, make sure that the schedules are staggered to prevent the server from overloading. When you turn on the Linux tasks, you must type the Novell Mirror Credentials and the Red Hat Network access credentials. By default, all vendors and all channels are enabled. You can customize the settings later on the appropriate Import Patch Data pages. 3 (Optional) Configure the notification options. If you enable administrator notifications, you must also configure the SMTP server settings. You can configure SMTP settings on the **Settings > Notification Server > Notification Server Settings** page. 4 On the next page, configure the assessment scan and update installation schedules or leave the default ones. 5 Click **Schedule patch**.	N/A
When a maintenance window is configured, the update installation does not run on the schedule.	If a maintenance window opens before the software update installation schedule, the schedule (including the **Start/End dates**) is disregarded and the software update gets installed before the scheduled time. This issue occurs when **Override Maintenance Windows settings** is not checked. This behavior is expected.	N/A
A log file is created on the endpoint.	A log file is created on the endpoint that lets you troubleshoot patch installation issues for the particular computer. The log file location is as follows: `%ALTIRIS_AGENT_INSTALL_FOLDER%\Agents\PatchMgmtAgent\`	N/A

Table 8-6 Other things to know *(continued)*

Issue	Description	Article link
Integrating Patch Management Solution with IT Analytics solution.	IT Analytics solution provides the reports that display patch management data. By default, users with **Patch Administrator** role do not have access to these reports. To grant access, add the **IT Analytics Users** role to the users. For more information, see the IT Analytics documentation.	N/A
Interaction with the Windows Update service.	Installing software updates on Microsoft Windows Vista or later operating systems fails if the Windows Update service's startup type is set to **Disabled**. The service's startup type must be set to **Automatic** or **Manual** — when a software update is installed, it starts the service. The service is not stopped after the installation is complete. If you want to stop the service, you can run a post-deployment task. The Altiris Real-Time System Manager solution has a **Service Management** task that you can use.	N/A
CPU usage highly increased during PMImport task, if the SQL database is not installed on a separate server.	Multiple code optimizations for Import operations are designed to use all CPU resources. If you want to reduce the increased CPU usage on Notification Servers, which also hold the SQL database, you can use the following workarounds: ■ Use SQL software performance settings to limit CPU usage. ■ Schedule task to run during non-business hours. ■ Use registry settings to set the **WindowsMaxWorkerThreads** count that is used by the task, equal to the number of processor cores or lower, as follows: "WindowsMaxWorkerThreads"=dword:00000001 (change to count of processor's cores).	TECH210369

New virtual directory behavior

In the 7.5 SP1 release, the virtual directories and UNC shares are rearranged.

The changes in the virtual directories and UNC shares structure are as follows:

- The Software Update packages location folder is now shared, if it is not a system folder or a root disk.

  Warning: You need to be careful with the files stored at the Software Update package folder, because this folder is shared.

- You cannot set any system folder or a root disk as a **Location to** for the Software Update package.

- After you upgrade to the 7.5 SP1, the nightly scheduled **Package Refresh** task rearranges the virtual directories and UNC shares.
- If the Software Update package location folder that existed before the upgrade to 7.5 SP1 is a system folder or a root disk, the virtual directories for the packages that are located in that folder are not rearranged to a new structure. In this case, a warning message appears in the log during the upgrade.
  The Software Update package stays functional.
- If a system folder or a root disk is defined as a **Location to** for the Software Update package after the upgrade to 7.5 SP1, all the Software Update packages that are downloaded after the upgrade have the old structure of the virtual directories and UNC shares. When you download such a package, a warning message appears in the log.
  The Software Update packages remain functional.
- If a system folder or a root disk is defined as a **Location to** for the Software Update package after the upgrade to 7.5 SP1, and you run a **Check Software Update Package Integrity** task with the **Relocate the downloaded packages** box checked, the virtual directories and UNC shares structure does not change. In this case, a warning message appears in the log.
- For Windows Software Update packages, if you modified the Software Update package location manually before the upgrade, the folder two levels up from the Software Update package location is marked as a group root folder.

Warning: The group root folder is shared.

Symantec recommends that you copy the Software Update packages to the new Notification Server computer before you begin the off-box upgrade process. The packages need to be located on the new Notification Server computer at a location with the same path as on the old Notification Server computer.

After you copy the Software Update packages to the new Notification Server computer, make sure that the **Administrators** user group owns the folder, the subfolders, and files. If you do not copy the Software Update packages before the off-box upgrade, an error Unable to refresh the codebase information for package appears in the log for every missing package. The virtual directories for these packages are not rearranged to a new structure. The missing packages are recreated when you apply the Recreate Package function, or during the I**mport Patch Data** task with the enabled **Revise Software Update policies** option. In this case, the Software Update packages are downloaded to an old path, and the old virtual directories and UNC shares structure is created for them. The Software Update packages remain functional.

The following system folders are defined on the Notification Server computer:

- [0] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\START MENU\PROGRAMS\ADMINISTRATIVE TOOLS\
- [1] C:\USERS\{USER_NAME}\APPDATA\ROAMING\
- [2] C:\PROGRAMDATA\MICROSOFT\WINDOWS\START MENU\PROGRAMS\ADMINISTRATIVE TOOLS\
- [3] C:\PROGRAMDATA\
- [4] C:\USERS\PUBLIC\DESKTOP\
- [5] C:\USERS\PUBLIC\DOCUMENTS\
- [6] C:\USERS\{USER_NAME}\FAVORITES\
- [7] C:\USERS\PUBLIC\MUSIC\
- [8] C:\USERS\PUBLIC\PICTURES\
- [9] C:\PROGRAMDATA\MICROSOFT\WINDOWS\START MENU\PROGRAMS\
- [10] C:\PROGRAMDATA\MICROSOFT\WINDOWS\START MENU\
- [11] C:\PROGRAMDATA\MICROSOFT\WINDOWS\START MENU\PROGRAMS\STARTUP\
- [12] C:\PROGRAMDATA\MICROSOFT\WINDOWS\TEMPLATES\
- [13] C:\USERS\PUBLIC\VIDEOS\
- [14] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\
- [15] C:\USERS\{USER_NAME}\DESKTOP\
- [16] C:\WINDOWS\FONTS\
- [17] C:\USERS\{USER_NAME}\APPDATA\LOCAL\MICROSOFT\WINDOWS\HISTORY\
- [18] C:\USERS\{USER_NAME}\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET FILES\
- [19] C:\USERS\{USER_NAME}\APPDATA\LOCAL\
- [20] C:\USERS\{USER_NAME}\MUSIC\
- [21] C:\USERS\{USER_NAME}\PICTURES\
- [22] C:\USERS\{USER_NAME}\VIDEOS\

- [23] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\NETWORK SHORTCUTS\
- [24] C:\USERS\{USER_NAME}\DOCUMENTS\
- [25] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\PRINTER SHORTCUTS\
- [26] C:\USERS\{USER_NAME}\
- [27] C:\PROGRAM FILES\
- [28] C:\PROGRAM FILES (X86)\
- [29] C:\PROGRAM FILES\COMMON FILES\
- [30] C:\PROGRAM FILES (X86)\COMMON FILES\
- [31] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\START MENU\PROGRAMS\
- [32] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\RECENT\
- [33] C:\WINDOWS\RESOURCES\
- [34] C:\WINDOWS\RESOURCES\0409\
- [35] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\SENDTO\
- [36] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\START MENU\
- [37] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\START MENU\PROGRAMS\STARTUP\
- [38] C:\WINDOWS\SYSTEM32\
- [39] C:\WINDOWS\SYSWOW64\
- [40] C:\USERS\{USER_NAME}\APPDATA\ROAMING\MICROSOFT\WINDOWS\TEMPLATES\
- [41] C:\WINDOWS\

Chapter 9

Real-Time System Management

This chapter includes the following topics:

- Known issues

Known issues

The following are the known issues for this release.

The known issues are separated into the following groups:

- SOL/IDE-R issues
  See Table 9-1 on page 101.
- RTCI known issues
  See Table 9-2 on page 103.
- Other known issues
  See Table 9-3 on page 104.

Table 9-1 Known issues for SOL/IDE-R

Issue	Description	Article link
Non-Latin characters are not supported.	SOL terminal window does not support double-byte characters (Japanese, Chinese).	N/A
Intel AMT Serial-over-LAN does not work correctly with HP computers.	The following options must be configured in the ME BIOS advanced settings for Intel AMT Serial-over-LAN to work correctly with HP computers: ■ SOL Terminal Emulation Mode: ANSI ■ Disabled echo char: ON	N/A

Table 9-1 Known issues for SOL/IDE-R *(continued)*

Issue	Description	Article link
IDE-Redirection to floppy does not work on Dell client computers.	When the SOL/IDE-R session is used to remotely boot a Dell client computer from a physical floppy diskette that is inserted into a floppy drive on the Notification Server computer, or from a binary floppy image file, the client computer performs a restart but does not load the operating system. On the client computer's monitor, the message `Attempting remote IDE boot` appears, but the Real-Time System Manager's terminal window remains blank until the session is terminated. This is a known issue with Dell computers (tested on Dell OptiPlex 745c). Workaround: Start the client from other media (physical CD-ROM, DVD-ROM, or ISO image file).	N/A
`SOL session terminated` error message appears when establishing a remote SOL connection to a computer.	If a SOL session window is already opened for a computer, you must close it before establishing a new remote SOL connection to the computer. Otherwise, following error message may appear: `SOL session terminated`.	N/A
SOL and IDE-R disabled in the target computer's BIOS.	When SOL and IDE-R are disabled in the target computer's BIOS, the controls for these options on the **Intel AMT Settings** page (**Task progress window and remote control** and **Redirect to optical/floppy drive or image on a server**) are not disabled.	N/A
IDE-R session to MS-DOS boot image does not work correctly with certain HP client computers.	IDE-R session to an MS-DOS boot image may not work correctly with the managed HP client computers that have BIOS versions earlier than 1.5. Workaround: Upgrade BIOS on the client computer.	N/A
Alt+<key> sequences do not transfer to client computer during SOL session.	When you use any Alt+<key> sequence on the keyboard during the Serial-over-LAN session, the controlled computer may not receive it.	N/A
Cannot install Windows using IDE-R on HP Compaq dc7700p system.	Due to SOL emulation limitations, installation of a graphical operating system through IDE-R can lead to a BSOD on some Intel vPro implementations and is not fully supported by Intel AMT 2.x products. The problem affects HP Compaq Business Desktop System BIOS for Intel vPro Technology (786E1 BIOS). Workaround: Download and install the latest BIOS/firmware update from the vendor's website.	N/A

Table 9-1 Known issues for SOL/IDE-R *(continued)*

Issue	Description	Article link
The first line of the terminal output is not displayed in SOL/IDE-R session.	When you establish a SOL/IDE-R session with HP computers with Intel AMT 2.5, the first line of the terminal output is not displayed in the remote console.	N/A
Ctrl+Alt+Del sequence does not work in the SOL session.	Ctrl+Alt+Del key sequence does not work in the SOL session established with Intel AMT 2.5 devices.	N/A
Function keys do not work in the SOL session.	If some of the F1-F10 keys do not work in the SOL session, use the <Esc>+1 - <Esc>+0 key sequence to emulate the function keys. This problem only occurs with certain BIOS firmware.	N/A
SOL/IDE-R session terminates after one minute when it is run by wireless interface.	On some hardware (HP, Fujitsu), the SOL/IDE-R session initiated by wireless connection terminates after 1 minute. This is a hardware limitation. To work around this issue, do the following: 1 In the Notification Server computer's registry, set the following DWORD value to *1*: *HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\Notification Server\ProductInstallation\ {13987439-8929-48d2-aa30-ef4bf0eb26a6}\InstantAMTPing*. 2 Restart the IIS.	N/A
One-to-many server IDE-R task fails if the IDE-R session is left active from the one-to-one real-time task and vice versa.	You must wait until the previous session is expired or terminate the session manually.	N/A
Boot redirection options not available for DASH computers.	**Real-Time View > Administrative Tasks > Hardware management > Redirection** options are not available when connected to a DASH computer. This issue is firmware-dependent. Upgrading DASH firmware can solve the problem.	N/A

Table 9-2 Known issues for RTCI/RTSM

Issue	Description	Article link
Unable to execute one-to-one power actions.	If the redirection privileges are disabled it is impossible to execute one-to-one power actions, such as power off or restart.	N/A

Table 9-2 Known issues for RTCI/RTSM *(continued)*

Issue	Description	Article link
Not possible to run out-of-band tasks on IPMI computers.	It is not possible to run one-to-many out-of-band tasks on IPMI computers. That is because the IP address of the IPMI management controller differs from the computers's IP address. Notification Server does not know the IPMI controller's IP. Running one-to-many out-of-band task is not possible on IPMI computers.	N/A
Restore State power action cannot restore S4 and S3 states.	The **Restore State** power action is not capable of putting computers into Stand-by (S3) or Hibernate (S4) states. Consequently, the **Restore State** power action turns off the computer (if needed) in an attempt to restore the Hibernate (S4) state and turns on the computer (if needed) to restore the Stand-by (S3) state.	N/A
Some Intel AMT inventory data is not collected.	The following Intel AMT inventory is not collected by the **Get Out-of-Band Inventory** task: ■ RTCI AMT Battery Serial Number ■ RTCI AMT Battery Manufacture Date	N/A

Table 9-3 Other known issues

Issue	Description	Article link
Error while performing power management operation `Reboot` command.	One-to-one and one-to-many **Reboot** power management command using WS-MAN connection executes with an error `Power management operation failed` on the UI, despite the fact that the computer successfully restarts. This problem is known for Dell Precision T3500 computers.	N/A
Not possible to connect to Intel AMT 5.0 using secure WS-MAN connection.	It is not possible to connect to Intel AMT 5.0 using secure WS-MAN connection. To solve this limitation, you need to upgrade the Intel AMT 5.0 firmware to the latest Intel AMT 5.2.	N/A
Unable to connect to Intel DASH computer configured in mutual authentication mode.	Secure connection, using the WSMAN protocol, to an Intel DASH computer that is configured in **Mutual authentication** mode is not supported.	N/A
IDE redirection does not work with "Kerberos" user.	When you are connected to a client using the "Kerberos" user, starting IDE redirection session can fail.	N/A

Table 9-3 Other known issues *(continued)*

Issue	Description	Article link
Firewall settings prevent WMI connection to a computer running Windows XP Service Pack 2.	If you provided valid WMI credentials, but cannot establish a WMI connection to a computer that is running Windows XP Service Pack 2 (WMI is not in the list of supported protocols on the Real-Time Consoles page), check the firewall settings on the target computer. The default configuration of the Windows Firewall program in Windows XP SP2 blocks incoming network traffic on Transmission Control Protocol (TCP) port 445. Configure the firewall to allow incoming network traffic on TCP port 445.	N/A
Firewall settings prevent remote connection to Windows Vista, 7, 8 or 8.1 client computers.	When using Real-Time System Manager to remotely connect to Windows Vista, Windows 7, Windows 8, or Windows 8.1 client computers, you must make sure that Windows Firewall is configured to allow remote Windows Management Instrumentation (WMI) connections on the client computer. To enable WMI connections on Windows Vista, in the Control Panel, click **Windows Firewall > Change Settings > Exceptions**, and then check **Windows Management Instrumentation (WMI)**. Additionally, for standalone WWindows Vista, Windows 7, Windows 8, or Windows 8.1 clients (not in a domain), you must disable the User Account Control (UAC). For example, to do this for Windows Vista, in the Control Panel click **User Accounts > Turn User account control on or off** and then uncheck **Use User Account Control (UAC) to help protect your computer**. Optionally, you can disable the UAC for the built-in administrator account (if you want to use this account for remote connection). To do this, in the **Control Panel > Administrative Tools > Local Security Policy** MMC snap-in, click **Local Policies > Security Options** and disable the **User Account Control: Admin Approval mode for Built-in Administrator account** policy.	N/A
Connection capabilities limited when connecting to computers that have multiple network cards.	Real-Time System Manager's connection to client computers that have more than one NIC (network interface card) has been improved. The following limitations still apply: ■ The Real-Time System Manager connection timeout is 10 minutes. ■ The Symantec Management Agent must have the Configuration Management Database (CMDB) updated with the new IP address after the client computer connects to the network.	N/A

Table 9-3 Other known issues *(continued)*

Issue	Description	Article link
One-to-many tasks cannot manage resources by an IP address.	To manage a computer from the **Real-Time** view one-to-one, you can enter an IP address and connect to the computer. One-to-many tasks do not work in this way. To run one-to-many tasks, the target computer's FQDN must be resolvable correctly from the Notification Server computer.	N/A
Cannot power off Intel ASF hardware from S3 state.	Some Intel ASF hardware does not support power off from the S3 state. You can try to turn on the computer and then run the turn off command again. Broadcom ASF does not have this problem.	N/A
PXE Boot does not work with some ASF hardware.	When in the **Real-Time** view you select the **Reboot** command and choose to boot from PXE, some ASF hardware fails to boot from PXE. This is a hardware limitation. HP with Broadcom ASF, DELL Precision T3400, and a few other computers are known to have this problem. You can try to turn off the computer and then turn on and boot from PXE.	N/A
Managed Service Provider configurations are not supported.	Both one-to-one and one-to-many tasks in the Real-Time System Manager software require a direct connection to the target computer that you want to manage. It is not possible to manage computers located behind NAT-enabled routers.	N/A
Graceful shutdown or restart returns an error on Microsoft Windows Vista, Windows 7, Windows 8, or Windows 8.1.	A `Graceful reboot or power off is not possible` error can appear when you check **Allow user to save data before power operation** and try to **Reboot** or **Power off** a Microsoft Windows Vista, Windows 7, Windows 8, or Windows 8.1 client computer. This occurs because one of the following: ■ The specified computer does not support a shutdown interface. ■ The caller does not have the required privilege to perform this operation. ■ The specified computer does not exist or is not accessible. ■ An invalid set of parameters was passed. ■ A shutdown has already been started on the specified computer. ■ A system shutdown has already been scheduled. ■ The system shutdown cannot be initiated because there are other users logged on to the computer. ■ The format of the specified computer name is invalid. You can uncheck **Allow user to save data before power operation** and try to perform a hard reset of the target computer, losing all unsaved data.	N/A

Table 9-3 Other known issues *(continued)*

Issue	Description	Article link
Not possible to update operating system properties on some computers.	It is not possible to update properties on the **Operating System** page in the **Real-Time** view if the target computer is running Microsoft Windows Vista (32-bit and 64-bit editions).	N/A
Only secure CIRA connections are supported.	Intel AMT computer management using CIRA is possible only with Intel AMT 4.0 and later computers that are configured to use TLS or TLS with mutual authentication.	N/A
Unable to connect to Intel DASH computer configured in mutual authentication mode.	Secure connection, using the WSMAN protocol, to an Intel DASH computer that is configured in **Mutual authentication** mode is not supported.	N/A
Setup and Configuration Server address is not displayed.	In the **Real-Time** view, on the **Intel AMT Configuration Mode** page, the setup and Configuration Server address is not shown for computers with Intel AMT version 2.6 and 4.0.	N/A
During upgrade, custom configuration of Network Filtering resets to default.	During the upgrade to 7.5 any custom filters of Network Filtering are reset to the default configuration. To keep using the custom setting you need to do the following: ■ On your NS Server, from the *\RTSM\Web\UIData* folder, copy the `CBFilters.bak` file. ■ Rename the `CBFilters.bak` file to `CBFilters.xml`. ■ Replace the original xml with the one containing the custom configuration.	N/A

Chapter 10

Software Management Solution

This chapter includes the following topics:

- What's new in this release
- Known issues
- Fixed issues
- Other things to know

What's new in this release

In Software Management Solution 7.5 SP1, the following new features are introduced:

Table 10-1 List of new features

Feature	Description
Improved Software Portal performance	Multiple code optimizations are implemented to speed up loading the software resources. Administrators may notice performance improvement by over 50%.
Improved Symantec Management Agent stability	Numerous fixes have been implemented to ensure greater stability of Symantec Management Agent.

Table 10-1 List of new features *(continued)*

Feature	Description
Software Library packages are located under one virtual directory	All packages from the Software Library are now located under one package share in IIS. The packages are marked and relocated into one package share in IIS, based on the **Nightly** schedule. **Warning:** The packages relocation fails in case the software package location folder, that existed before the upgrade to Software Management Solution 7.5 SP1 is a system folder or is not available during the upgrade procedure.
Agents and plug-ins can be installed during a maintenance window	Agents/Plug-ins rollout policies allow users to set installation during a maintenance window.
Additional way to create and target Managed Software Delivery policies	A Managed Software Delivery policy can be created for computers by dragging and dropping the software release on the target, which contains the corresponding computers. This will start a Managed Software Delivery policy wizard with prepopulated settings to target the corresponding computers. Dragging and dropping an existing Managed Software Delivery policy on the target, adds the corresponding computers to the list of computers, targeted by the policy.
Minor refactoring of the Managed software delivery policy UI	**Result-based actions** tab UI for the **Advanced options** in Managed software delivery policy is refactored.
Symantec Workspace Streaming Agent is installed with Software Management Solution.	A new package for Symantec Workspace Streaming Agent is distributed as part of Software Management Solution. For more information about installation and management of the Symantec Workspace Streaming Agent, see the *Installing the Workspace Streaming Agent* chapter and the *Managing the Workspace Streaming Agent* chapter in the *Workspace Streaming 7.5 SP1 Installation and Implementation Guide* at the following URL: http://www.symantec.com/docs/DOC7391

Known issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- General issues
  See Table 10-2 on page ?.
- Managed software delivery issues

See Table 10-3 on page ?.

- Software Portal issues
  See Table 10-4 on page ?.
- Hierarchy and replication issues
  See Table 10-5 on page ?.
- Non-Windows-specific issues
  See Table 10-6 on page ?.
- Software Management Framework issues
  See Table 10-7 on page ?.
- Other issues
  See Table 10-8 on page ?.

Table 10-2 General issues

Issue	Description	Article link
If you import custom software resources to `\\<NS>\NSCAP` folder, it is removed during upgrade.	If you import custom software resources to `\\<NS>\NSCAP` UNC share, and then upgrade Symantec Management Platform, the software is removed during the process.	N/A
Symantec Management Agent and Software Management Plug-in require upgrade to run Managed Delivery Policies and Quick Delivery tasks under specific user credentials.	After upgrade from IT Management Suite 7.0, previous versions of Symantec Management Agent and Software Management Plug-in may fail to run Managed Delivery Policies and Quick Delivery tasks under specific user credentials. Workaround: Upgrade Symantec Management Agent and Software Management Plug-in or run Managed Delivery Policies and Quick Delivery tasks using Symantec Management Agent credentials.	N/A
Unable to generate a command line for a package from a Software Library.	If the Software Library is specified as a source for a package containing large files, while editing an existing software resource, the command lines are not generated for this software resource.	N/A
Software discovery creates second software resource for software resource, imported from MSI.	If after running the Software Discovery task or gathering software inventory, Software Catalog duplicates previously imported software resources as newly discovered software resources, this means, that the corresponding imported MSI files contained different software keys. Workaround: To fix the issue, run the Merge Duplicate Resources scheduled task. If this task does not fix all issues, merge the software resources manually.	N/A

Table 10-3 Managed software delivery issues

Issue	Description	Article link
Managed Software Delivery policy fails to install software into a virtual layer on Windows 7 Embedded.	Managed Software Delivery policy may fail to install a software application into a virtual layer on computers running Windows 7 Embedded operating system.	N/A
Managed Software Delivery policies stay in the detection check state after upgrade.	If Managed Software Delivery policies stay in the detection check state on the client computer for a long time after upgrade, then they may not get executed. Workaround: To fix this issue, restart the affected client computer or the corresponding Symantec Management Agent.	N/A
Dependent software installation issue.	If Managed Software Delivery policy is created for a software, which has a dependency on another software, using **Managed Software Delivery** wizard, where on the **Specify dependencies and updates** page the **Verify dependencies** option is checked and the software resource option is unchecked for the corresponding software, the dependent software is not installed even if the dependency option is later checked in the policy settings. Workaround: To fix the issue, remove the software resource from the Managed Software Delivery policy and add it again.	N/A
Managed Software Delivery policies and Quick Delivery tasks fail to run from a directory on the Notification Server computer.	Managed Software Delivery policy or a Quick Delivery task fail with a 1619 error code, if the following conditions are met: ■ There are no package servers in an environment; ■ A software resource is imported from a Notification Server; ■ The **Use the following settings to download and run** option is checked; ■ The **Download and run locally if bandwidth is above** is unchecked; ■ The **Run from server if bandwidth is above any connection speed** is checked; ■ The **Current logged-in user** option is checked on the Run Options settings.	N/A
File Version detection check does not support the %user name% environment variable.	When running a Managed Software Delivery policy under **Currently logged in user**, the file version detection check fails to detect a file, which is located under the %user name% folder. Workaround: To fix the issue, in the file location path, use the %useprofile% environment variable, which points to the same folder.	N/A

Table 10-3 Managed software delivery issues *(continued)*

Issue	Description	Article link
Registry Key/File Path to File Version and **Registry Key/File Path to Product Version** rules do not support environment variables.	When running a Managed Software Delivery policy under **Currently logged in user**, the **Registry Key/File Path to File Version** and the **Registry Key/File Path to Product Version** detection rules fail to detect a file, if the path is specified using environment variables.	N/A
Client computer restarts on completing the software installation may confuse the computer users in case of different settings, specified by multiple users.	If multiple users log in locally or remotely to the client computer, on which a software resource is installed by a Managed Software Delivery Policy, and specify different settings, when prompted to restart the computer after the software installation is complete, the following situations may occur: ■ If a client computer user snoozes the computer restart, after a software resource is installed by a Managed Software Delivery policy, computer can only restart, when this user is logged in again. If another user logs in to the same client computer and selects to restart the computer after the installation is complete, the computer does not restart. ■ If a user has accepted computer restart, but it was snoozed by another user, or the maintenance window has not started yet, the computer will then restart unexpectedly for the first user, when the snooze period, specified by another user expires or the maintenance windows starts.	N/A

Table 10-4 Software Portal issues

Issue	Description	Article link
Software Portal publishing permissions are incorrectly migrated during upgrade from Software Management Solution 6.x	When migrating from Software Management Solution 6.x the Software Portal publishing permissions for a software resource change their status from **Approved** to **Requesting Approval**.	N/A

Table 10-5 Hierarchy and replication issues

Issue	Description	Article link
Managed Delivery policy, which contains a software resource with applicability checks, is not replicated to the Child Notification Server.	If on the Parent Notification Server you create a Managed Software Delivery policy, which contains a software resource with Applivability checks, apply it to client computers, assigned to the Child Notification Server and then run an emergency update on that policy, the policy is not replicated to the Child Notification Server Workaround: To fix the issue, run the differential replication task.	N/A

Table 10-6 Non-Windows-specific issues

Issue	Description	Article link
A false-positive status for a software package on a Mac client computer may be reported, if the user cancels the software interactive installation.	If a user of a Mac client computer cancels a Quick Delivery task or a Managed Delivery task, which has an interactive install, the success execution event is sent to the Notification Server, leading to a false-positive status for this installation. At the same time, the software scan for the Quick Delivery task and the detection check for the Managed Delivery task provides the correct information.	N/A

Table 10-7 Software Management Framework issues

Issue	Description	Article link
Computer resource information is lost, when imported from another Notification Server.	If you import computer resource information from an XML file, exported from another Notification Server, the computer resource information related to installed software in the Resource Manager is lost.	N/A
Source Path Update and Windows Installer Repair tasks fail on Windows Server 2012 R2 Core.	Source Path Update and Windows Installer Repair tasks fail with error code - 1073741515 on computers, running Windows Server 2012 R2 Core operating system.	N/A
A Managed Software Delivery policy only logs off a single user session when there are multiple active or disconnected terminal sessions.	The **Log off user** option in the **Managed Software Delivery** policy logs off only a single session rather than all sessions when multiple sessions are active. For more information, see topics on Results-based actions settings in Software Management Solution in the *IT Management Suite Administration Guide* at the following URL: http://www.symantec.com/docs/DOC7220 Workaround: Use the **Log off** option available with the **Restart Computer** task to successfully log off every session.	N/A

Table 10-7 Software Management Framework issues *(continued)*

Issue	Description	Article link
Files in the **File Inventory** tab may be overwritten.	Files in the **File Inventory** tab are overwritten if a software resource is moved to **Managed Software** and metering is turned on for this software resource.	N/A
Quick Delivery tasks fail to execute by timeout when maintenance window is set up on clients.	If you create a Quick Delivery task and the task times out before the maintenance window is activated on the client, the task fails. By default, a task times out after 300 minutes. On the **Task options** tab of the Advanced settings, you can change when a task ends.	N/A
Applications with large installation paths fail to execute.	With a Managed Software Delivery policy or Quick Delivery task, applications with large installation paths fail to execute.	TECH133459
When creating a package by ASDK command lines may get not generated for the package.	When creating a package by ASDK **AutoGenerateCommandLines** parameter set to **True**, no command lines are generated for the package.	N/A
Unable to add one large file or a very big number of small files, estimating around 2 GB in total, while editing a software resource.	If you add one large file or a very big number of small files, estimating around 2 GB in total, the procedure will fail with errors in the Notification Server computer log file, while editing a software resource.	N/A
Installation error code descriptions are not migrated when upgrading from Software Management Solution 7.0.	Modified installation error code descriptions are reset to default values, after upgrading from Software Management Solution 7.0.	N/A
Weak ACL for a shared location, which is used for the Software Library, may lead to issues with Software Library data safety.	Setting weak ACL, such as "Everyone", for a shared location, which is used for the Software Library, may lead to intentional or unintentional loss of Software Library data or lack of storage on the corresponding server. Workaround: To prevent the issues, set strong ACL for UNC path, which leads to the Software Library repository.	N/A
Importing packages, if package files contain sensitive information in unencrypted form, may lead to a possibility of information disclosure threat.	When importing software packages using Import Software wizard, package files can be read by an unauthorized party during data transfer from package store to the Notification Server computer. If package files contain sensitive information, such as passwords inside scripts, in unencrypted form, then such software import can be a subject to information disclosure threat	N/A

Table 10-7 Software Management Framework issues *(continued)*

Issue	Description	Article link
Migrated software components are not merged with newly discovered software components if those components have separate 32-bit and 64-bit versions.	After upgrading to Software Management Solution 7.5, software component duplicates appear in Software Catalog, after running Software Discovery for those components which have 32-bit and 64-bit separate versions	N/A

Table 10-8 Other issues

Issue	Description	Article link
"Windows computers with installed Software Management plug-in" filter does not support Legacy mode.	If you enable Legacy Agent Communication mode after you upgrade Notification Server, the "Windows computers with installed Software Management plug-in" filter along with the tasks and policies, based on this filter does not work, unless the Software Management plug-in is up-to-date.	N/A
Virtual layers stop working after uninstalling the SWV agent from the client computer, until you restart this computer.	You must must restart the client computer after you uninstall the Symantec Workspace Virtualization Agent from it using the "Uninstall SWV agents" policy. Otherwise, the software applications, installed into virtual layers may stop working correctly.	N/A
Virtual Composer version in the software resouces and rules remain unchanged after upgrade.	The version of the Virtual Composer in the software resource package remains unchanged, after upgrading to Software Management Solution 7.5 SP1. Detection and applicability rules, based on the Virtual Composer version must be updated manually.	N/A
Resource items for components deleted after upgrade appear in Software Component resource view.	Software Virtualization related resource items for deleted packages appear in the Software Component Type Organizational Group, after upgrade to Software Management Solution 7.5 SP1.	N/A
Custom tasks or policies, based on SWV agent packages, require manual recreation after upgrade.	If you have custom Managed Delivery policies, Quick Delivery tasks or Package delivery tasks, which use Symantec Workspace Virtualization Agent, you have to manually recreate such tasks or policies after upgrade to Software Management Solution 7.5 SP1.	N/A
If the Software Library is not accessible during the upgrade, software packages are not grouped on the IIS web server.	If the Software Library is inaccessible during the upgrade to Software Management Solution 7.5 SP1, software packages are not grouped properly on the IIS web server.	N/A

Table 10-8 Other issues *(continued)*

Issue	Description	Article link
Software resource “conflicts with” association is lost after detailed export – import procedure.	If you run a Detailed Export for a software resource, which has a "conflicts with" association, then this association is not displayed after importing the resource from the XML file.	N/A
An error appears, when trying to install Wise Toolkit.	An error appears, when trying to install Wise Toolkit on a server with installed Software Management Solution 7.5 as a result of the end-of-life of Wise Package Studio.	TECH210284

Fixed issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 10-9 Fixed issues

Issue	Description	Article link
Full inventory is required to gather missing uninstall string for a software resource.	The uninstall string from Add/Remove programs for a software resource could be missing from the inventory, gathered by the previous versions of the Symantec Management Agent. After the upgrade, delta inventory does not gather this information.	N/A
Compliance reports still display computers after they are removed from the policy target.	If a computer, to which a specific Managed Software Delivery policy is applied, is displayed in any of the corresponding compliance reports, it will still be displayed in these reports after it is removed from the policy target.	N/A
Prerequisite checks are skipped during the installation of a single item from the MPKG files.	If a single item is specified from an MPKG file for installation on a Mac OS client computer, then the prerequisite checks are ignored during the installation on the client computer.	N/A
Incorrect association results for two Notification Servers in a hierarchy in a certain situation.	Consider two Notification Servers in a hierarchy. This problem occurs if the parent and child have the same software resource imported but have different software products associated with the resource. When you perform replication from the parent to the child under these circumstances, the affected software resource on the child shows an incorrect association. Instead of showing one association from the parent Notification Server, the affected software resource shows two associations: one from the parent and one from the child.	TECH176457

Table 10-9 Fixed issues *(continued)*

Issue	Description	Article link
The **Software Data Provider Status** report does not show results.	When you add or run data providers and then try to view the status of the data providers using the **Software Data Provider Status** report, the report does not show results.	N/A
Software Components do not replicate using **Replicate Now**.	Replication of software components does not work from a parent or child Notification Server when you use **Replicate Now** in the following situations: ■ In the **Software** view, when you use the right-click menu **Hierarchy > Replicate Now** on either **Software Releases** or **Software Updates**. ■ In the **Manage** menu, select **All Resources**, and right -click on a software component. From the right-click menu select **Hierarchy > Replicate Now**.	N/A
An incorrect version is reported for Microsoft Internet Explorer 8.	When you run **Collect Full Inventory** on a client computer with Microsoft Internet Explorer 8 installed, the version is incorrectly displayed in the inventory report.	N/A
Software resource associations of a software component to file are not present if an application is installed on a client computer for a specific user.	Consider a software application that is installed on a client computer by a specific user. A **Collect Full Inventory** is then run for that client after a different user logs in to this computer. In this situation, the resource associations of the software component to file is lost for this software resource. The problem occurs because Software Discovery tries to load values from a user-specific registry. However, it is unable to load those values because the specific user is not logged on.	N/A
Users with enabled required privileges and permissions cannot create delivery tasks.	Level 1 Worker with enabled required privileges and permissions cannot create a Quick Software Delivery task and a Managed Software Delivery Policy	TECH195077
The remediation schedule on a Managed software delivery policy on the child server is over-written during replication.	Even with Hierarchy Editable Properties (HEP) enabled, the remediation schedule on a Managed software delivery policy on the child server is over-written with the parent server schedule during replication.	TECH212998
A Managed software delivery policy may return an empty software screen.	A Managed software delivery policy returns an empty software screen, if you remove a command line or a package from the software resource, which is used in the policy.	N/A
In Software Portal, by default, Software is not sorted by name.	In Software Portal, by default, the contents of the **Request software** table is not sorted by software name.	N/A

Table 10-9 Fixed issues *(continued)*

Issue	Description	Article link
Agent fails to update the package after it is updated during a Quick Delivery task or a Package Delivery task execution.	If a software package executable is replaced by another file with the same name, Software Management Framework Agent fails to update local cached version on the client computer and uses the old package version during a Quick Delivery task or a Package Delivery task execution.	N/A
Heavy Software Portal usage considerably affects the Notification Server performance.	Heavy Software Portal usage leads to degrading Notification Server performance due to high database growth rate.	N/A
Software portal page request times out while loading.	Software portal page request times out due to long Active Directory membership analysis.	TECH174477
Errors appear in logs after running the Software inventory or Hardware inventory tasks.	Errors, related to Software Management Framework Agent and SMFAgent.dll, appear in logs after running the Software inventory or Hardware inventory tasks.	N/A
Managed Software Delivery policies cannot be run from servers on client computers running Windows Vista or Windows 7.	If the **Run from server if bandwidth is above some speed** advanced option is checked for a Managed Software Delivery download settings, the policy will fail with a 1619 error code on the client computers running Windows Vista or Windows 7 operating systems.	N/A

Other things to know

The following are the other things to know about this release.

Table 10-10 Other things to know

Issue	Description
Old **AddRemoveProgram** data class entries are displayed in the Resource Manager after the corresponding software is upgraded on the client computers.	If a client computer software, for which the data is already gathered by the **Collect full inventory** task, is upgraded, old entries in the AddRemoveProgram data class are visible in the Resource Manager, even after running the **Collect full inventory** task on this client computer. Workaround: To fix the issue, run the **Collect full inventory** task on this client computer once again.

Table 10-10 Other things to know *(continued)*

Issue	Description
Java Update software component is not added into the Software Catalog after running the Software Discovery task.	Java 6 Update software component, which is installed on the client computer, is not added into the Software Catalog after running the Software Discovery task. This happens, because Java 6 Update software component has association with Java(TM) 6 Unmanaged software product, which is added by the Inventory Solution.
If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails.	If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails. The reason the installation fails is that the software starts to install while a user logoff is still pending.
The support of **Run from server if bandwidth is above some speed** setting is limited in CEM mode.	The usage of this setting on Internet-managed client computers is limited as follows: ■ If the setting is enabled for a Quick Delivery task or a Package Delivery task, these tasks will fail with timeout error, unless the client computer connects remotely or locally with corresponding bandwidth to the Notification Server computer or Package Server, to which it is assigned, before the task timeout period is reached. ■ If the setting is enabled for a Managed Delivery policy, the policy will not run, until the client computer connects remotely or locally with corresponding bandwidth to the Notification Server computer or Package Server, to which it is assigned, before the task timeout period is reached.
Computers in CEM mode cannot be turned on if necessary.	The **Power on computers if necessary** compliance setting is not supported for Internet-managed client computers due to limitations of remote power management technology.
Managed Software Delivery policies and Quick Software Delivery tasks execution requires Symantec Management Agent upgrade.	Due to significant changes in this component, Symantec Management Agent has to be upgraded to version 7.5 in an environment with hierarchy, to execute Managed Software Delivery policies and Quick Software Delivery tasks
Source Path Update execution requires Symantec User credentials.	Source Path Update will only work under Symantec User Credentials.

Table 10-10 Other things to know *(continued)*

Issue	Description
The status of the Quick Delivery tasks for software resources with EXE files, which contain MSI packages, does not reflect the status of the embedded MSI package installation.	Tasks and policies allow you to use software packages with EXE executable files, which contain MSI components. The logic behind such tasks only monitors the execution of the initial EXE file, which calls the MSI component. Once the embedded MSI is triggered, the result of the task or policy is considered to be successful. This may lead to confusing situations, in case the embedded MSI file fails to complete, particularly, when you use Quick Delivery tasks, which do not utilize detection checks. For example, if you try to install an executable with Adobe Reader in silent mode, using a Quick Delivery task on a client computer running Windows 7 Embedded, the installation may fail, without returning an error code, while the Quick Delivery task status returns successful completion of the executable file. Symantec recommends you to use MSI software packages instead of EXE files and policies with detection checks instead of Quick Delivery tasks, where possible, to make sure receive accurate and detailed information about the software installation process.
Tasks and policies may fail to access UNC source locations in complex network environments..	Windows Installer Repair task, Quick Delivery task, Package Delivery task and Managed software delivery policy may fail to access the UNC source location, which contains the software package, in an environment, where Notification Server, package server and client computers do not reside in the same domain. To ensure access to such packages, use the agent connectivity credential to connect to download resources. For more information setting up access to the Package Server, see the *Enabling access to a package at a UNC source location* section in the *IT Management Suite Administration Guide* at the following URL: http://www.symantec.com/docs/DOC7220

Chapter 11

Symantec Endpoint Protection Integration Component

This chapter includes the following topics:

- About Endpoint Protection Integration Component
- Known issues

About Endpoint Protection Integration Component

Endpoint Protection Integration Component combines Symantec Endpoint Protection with your other Symantec Management Platform based products. You can inventory computers, deliver software and patches, and deploy new computers. You can also back up and restore your systems and data, manage data loss prevent (DLP) agents, and manage Symantec Endpoint Protection clients. You can do this work from a single, web-based Symantec Management Console.

Note: In this release of IT Management Suite 7.5 SP1, the Endpoint Protection Integration Component 7.5 is packaged. No new features are introduced. For more information on the Endpoint Protection Integration Component 7.5 Known Issues See "Known issues" on page 121.

Known issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link:

Table 11-1 Known issues

Issue	Description	Article Link
Collecting Antivirus Inventory for F-Secure Anti-Virus 2012.	The **Antivirus inventory** task is unable to collect inventory for F-Secure Anti-Virus 2012.	N/A
Support for McAfee 2011 v10.5.227 in JP/CS/CH/KN languages.	Endpoint Protection Integration Component does not support McAfee 2011 in the following languages: ■ Chinese Simplified ■ Japanese ■ Korean ■ Chinese Traditional	N/A
Endpoint Protection Integration Component task issues with Symantec Endpoint Protection 12.1.	Endpoint Protection Integration Component scan tasks such as full scan and Quick Scan fail on Symantec Endpoint Protection 12.1.	N/A
Endpoint Protection Integration Component repair task execution.	Endpoint Protection Integration Component repair task does not execute for the supported Symantec Endpoint Protection versions except Symantec Endpoint Protection 11.0.7072.1031.	N/A
Registry entries and folders.	Few registry entries and folders are present even after you uninstall the existing antivirus. The count of these entries and folders varies for the antivirus solutions.	N/A

Table 11-1 Known issues *(continued)*

Issue	Description	Article Link
Uninstallation and inventory of localized antivirus software.	The Endpoint Protection Integration Component 7.5 does not support inventory or uninstallation of the localized versions of the following antivirus software: ■ F-Secure AV 2012 ■ F-Secure IS 2012 ■ F-Secure AV for workstations 9.30 ■ Kaspersky Endpoint Protection Integration Component 7.5 by default supports the uninstallation and inventory of the following localized antivirus software: ■ ESET NOD32 5.0 ■ ESET SMART SECURITY 5.0 ■ CA Antivirus Plus 2010 ■ McAfee Antivirus Plus 2012 ■ McAfee Total Protection 2012 ■ Trend Micro Office Scan Client 10.5 ■ F-Secure AV for Windows Servers 9.20 ■ SAVCE 10.1.9000.1 ■ SOPHOS Antivirus 9.7 Endpoint Protection Integration Component 7.5 supports the uninstallation of the following localized antivirus software: ■ MS Forefront Endpoint Protection 2010 ■ SAVCE 10.1.9000.9	N/A
32-bit and 64-bit package.	If a 32-bit package is selected for installation on a 64-bit computer, or a 64-bit package is selected for installation on a 32-bit computer, then the migration job fails	N/A
Power Sensitive Malware Scanning and Remote Machine Repair via IDER and SERT tasks are not supported on CEM environment.	The **Power Sensitive Malware Scanning** and Remote Machine Repair via IDER and SERT tasks do not work in CEM environment as the **Power On** task is not supported on the CEM environment.	N/A
Support for uninstallation of Kaspersky Antivirus.	The Symantec Endpoint Protection Integration Component 7.5 does not support the uninstallation of Kaspersky antivirus.	N/A

Table 11-1 Known issues *(continued)*

Issue	Description	Article Link
Incorrect task status is displayed on the Jobs and Tasks page.	The Jobs and Tasks page displays incorrect status for the **Migrate computers to latest Symantec Endpoint Protection Client** task. Following is the workaround for this issue: Before you execute the **Migrate computers to latest Symantec Endpoint Protection Client** task, uncheck the following: ■ **Restart the computer after the uninstall of the previous anti-virus software** ■ **Restart the computer after the installation of the Symantec Endpoint Protection Clients** Click **Save changes**.	N/A
The **Patch Vulnerability Assessment Scan** task fails on the client computer.	The **Patch Vulnerability Assessment Scan** task fails on the client computer with COM Exception and displays the error code 10010, when you execute the task with SEP Full Virus Scan Client Task.	TECH216177

Chapter 12

Virtual Machine Management

This chapter includes the following topics:

- What's new in this release
- System requirements
- Installing
- Supported hypervisors
- Known issues
- Fixed issues
- Other things to know

What's new in this release

In Virtual Machine Management 7.5 SP1, the following new features are introduced:

Table 12-1 List of new features

Feature	Description
Support for latest versions of the guest operating systems.	Now, Virtual Machine Management supports the following latest versions of the guest operating systems: ■ Windows 8.1 ■ Windows Server 2012 R2 ■ RHEL 5.10 ■ RHEL 6.5 ■ SLES 11 SP3 ■ Apple OS X 10.9 - Mavericks
Support for latest versions of the hypervisors.	Now, Virtual Machine Management supports the following latest versions of the hypervisors: ■ VMware ESXi 5.5 ■ Microsoft Hyper-V 2012 R2 ■ VMware vCenter 5.5 Virtual machines that are created under these hypervisors support latest operating systems.
Improved overall performance, scalability, and reduced tasks queues while performing various VMM tasks.	Now, Virtual Machine Management code is optimized to simultaneously execute multiple tasks on a task server. The tasks that are executed on the same virtual resource are executed synchronously. Simultaneous execution of multiple tasks provides following advantages: ■ Improved performance The new design reduces the overall tasks turnaround time. This results in performance gain in the tasks such as scheduled inventory tasks. ■ Higher scalability Now, you can assign more than one host or virtual machine to the same task server and initiate multiple tasks simultaneously without worrying about the timely completion of those tasks. ■ More reliability Simultaneous execution of multiple tasks helps in reducing the task queues and the task timeout-related failures. This results in reducing ambiguity and makes the task execution more reliable.
Support for latest versions of IE browser.	Now, Virtual Machine Management supports IE10 and IE11 browsers in compatibility mode to leverage the features that are provided by these latest IE browsers.
Pre-populated drop-down list for better usability.	While creating the **Deploy VM** task from the **Manage > Jobs and Tasks > System Jobs and Tasks > Virtual Machine Management** menu, now instead of typing-out the values, you can use the user-friendly drop-down lists to specify the value for the **Source Host Name** and **Template Name** fields.

Table 12-1 List of new features *(continued)*

Feature	Description
Improved response time of the tree view on the Virtual Machine Management portal page.	Virtual Machine Management code is optimized to reduce the loading time of the tree view on the Virtual Machine Management portal page. Now, the tree view page quickly loads the virtual environment with a large number of hosts and virtual machines.
Modification in the installation of the Virtual Machine Management Task Server Plug-in- Install policy.	Now, Virtual Machine Management Task Server Plug-in Install policy is, by default, roll out only on the Notification Server computer on which the task service is installed; the plug-in policy does not automatically roll out on all the task servers to prevent unwanted installation of this plug-in. You can find this policy on the **Settings > Agents/Plug-ins > Virtual Machine Management > Virtual Machine Management Task Server Plug-in - Install** page. Here, a new filter **Local NS computer with Task Service Installed** is added to list the local NS computer with the task service is installed. If you want to roll-out the VMM Plug-in install policy on a remote task server then you must select the respective targets in the install policy and run that policy. The policy installs the Virtual Machine Management Task Server Plug-in on your task server.

System requirements

Virtual Machine Management 7.5 SP1 requires the following software to be installed:

- Symantec Management Platform 7.5 SP1.
  When you install Virtual Machine Management using Symantec Installation Manager, the Symantec Management Platform is installed automatically.

The operating systems that are supported by the Symantec Management Platform are also supported by Virtual Machine Management.

For more information, see the product support matrix at the following URL:

http://www.symantec.com/docs/HOWTO9965

Installing

Install the solutions and components in the following sequence:

- Symantec Management Platform 7.5 SP1
- Deployment Solution 7.5 SP1
- Symantec Virtual Machine Management 7.5 SP1

Supported hypervisors

The following are the hypervisors supported in Virtual Machine Management 7.5 SP1:

- ESX 4.0
- ESX 4.1
- ESXi 4.0
- ESXi 4.1
- ESXi 5.0
- ESXi 5.1
- ESXi 5.5
- Hyper-V (Win 2K8 R2 enterprise)
- Hyper-V (Win 2K8 R2 SP1)
- Hyper-V (Win Server 2012)
- Hyper-V (Win Server 2012 R2)

vCenter 4.0, vCenter 4.1, vCenter 5.0, and vCenter 5.1, and vCenter 5.5 are also supported. They can be used to manage ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, and ESXi 5.5.

Known issues

The following are known issues for this release. If additional information about an issue is available, the issue has a corresponding Article link.

Table 12-2 Known issues in Virtual Machine Management 7.5 SP1

Issue	Description	Article Link
Base or old snapshot disk files, which are associated with a virtual machine, can be deleted or used as existing disk for new virtual machines.	Base or old snapshot disk files that are associated with the virtual machines and have at least single snapshot then they can be deleted or used as existing disk for new VM. These virtual machines include any Hyper-V VM or VMs whose exiting disks are used in ESX servers.	N/A

Table 12-2 Known issues in Virtual Machine Management 7.5 SP1 *(continued)*

Issue	Description	Article Link
Some VMs do not appear in the 'Inv_Vm_Guest' table.	Some VMs do not appear in the 'Inv_Vm_Guest' table after a Network Discovery task due to reasons like duplicate VM or template name exists under same host or VM\template with duplicate IP address. VMs do not appear in the left pane on the VMM portal, but do exist in the vSphere client. As a result, you cannot run any VMM tasks. The VMs do appear in ND logs.	N/A
Network Discovery task is not running on vCenter 4.0, but it is running on other Hypervisors after Microsoft patch installation.	The Network Discovery tasks are failing on vCenter 4.0, but they are running on other Hypervisors after Microsoft patch installation. This issue is happening because the vCenter 4.0 certificate is using 512-bit RSA keys. To work around this issue, use vCenter certificates with a minimum RSA key length as 1024. Alternatively, you can execute the command below on the task or NS server and set the minimum allowed RSA key length to 512. `certutil -setreg chain\minRSAPubKeyBitLength 512`	kb/2661254
Run Inventory task is failing due to protocol issues.	The Run Inventory task is failing due to protocol issues. To work around this issue, it is recommended that any discovery tasks that include vCenter servers in their scan range must use a connection profile where the VMware protocol is enabled and include the corresponding vCenter credential information. Be aware that enabling the VMware protocol in tasks with large scan ranges can take considerably longer to execute. You should consider excluding vCenter servers from these tasks so the VMware protocol does not need to be enabled for them, thus avoiding unsuccessful attempts to use the VMware protocol on a wide range of nodes. Instead, you can create vCenter-specific discovery tasks, where the individual vCenter servers are identified and the tasks use a connection profile where the VMware protocol as well as any other protocols needed to communicate to that server are enabled.	N/A
No operating system is displayed on the portal page.	On the **Virtual Machine Management** portal page, if you click a virtual machine on a Hyper-V server, the portal page does not display any operating system.	N/A
Capacity of the unassociated virtual disk is not displayed on the portal page.	On the **Virtual Machine Management** portal page, if you select an ESX server, the capacity of the virtual disk is not displayed if the disk is not associated with any virtual machine.	N/A

Table 12-2 Known issues in Virtual Machine Management 7.5 SP1 *(continued)*

Issue	Description	Article Link
Error displayed when you run a network discovery task on multiple ESX computers with the same name.	When you run a network discovery task on multiple ESX computers with the same name consecutively, the task updates the same resource entry. It does not create a separate resource entry for every ESX server.	N/A
Creation or deletion of virtual disks.	For the successful creation or deletion of virtual disks on the hosts, which are managed and discovered by a vCenter, the credentials for the hosts and respective vCenter must be the same.	N/A
Limitations to the Add host function.	On the **Virtual Machine Management** portal page, if you want to add a host, only the default connection profiles work.	N/A
The Virtual Machine Management portal page does not show edited data.	The Virtual Machine Management portal page does not show the edited data of your virtual resources. After you successfully perform any of the Virtual Machine Management tasks, the information on the **Virtual Machine Management** portal page is not updated. To work around this issue, on the **Virtual Machine Management** portal page, in the left pane, click the **Refresh** symbol to refresh the page and to see the edited data.	N/A
The data on the Virtual Machine Management portal page is not updated after you delete any virtual resources.	After you manually delete a virtual network, virtual disk, or snapshot on the host server, the resources are still displayed on the **Virtual Machine Management** portal page. To work around this issue, run the VMM inventory task to get the updated data.	N/A
The Virtual Machine Management portal page displays a virtual machine that is deleted manually in the list of virtual machines.	After you manually delete a virtual machine on the host server, the virtual machine still appears on the **Virtual Machine Management** portal page, in the list of virtual machines. However, if you create and run any Virtual Machine Management tasks on this virtual machine, these tasks fail. To work around this issue, run the discovery task on the host machine.	N/A

Fixed issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 12-3 Fixed issues in Virtual Machine Management 7.5 SP1

Issue	Description	Article link
You cannot delete the virtual resources and the snapshots that have special characters in their names.	You can successfully create virtual machines, virtual disks, virtual networks, and the snapshots that have special characters in their names. However, if you run the delete task to delete any of these resources, the task fails and does not delete the item.	N/A
All the guest operating systems are not available for selection while creating a virtual machine using the **Create VM** task.	While creating virtual machine using the **Create VM** task, the desired guest operating system cannot be installed due to unavailability of all the guest operating systems.	N/A
Virtual machine tasks are queued.	Virtual Machine Management tasks are queued because discovered virtual machines do not get assigned to site servers.	N/A

Other things to know

The following are things to know about this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 12-4 Other things to know

Issue	Description	Article link
Run the **Network Discovery** task and **Run Inventory** task, before viewing the **Orphaned Virtual Machine Report** report.	Before viewing the **Orphaned Virtual Machine Report** report, you must perform the **Network Discovery** task and **Run Inventory** task to get better results through the report.	N/A
Recommended Hyper-V ISO file paths.	In the **Create Virtual Machine** wizard, for a host, the ISO paths are available for selection only if they are under the parent folder or a root folder of the host In case of Hyper-V ISO files, the ISO paths are available for selection only in following scenarios: ■ ISO files are located under default Hyper-V disk path where `.vhd` files get saved. ■ ISO files, which are referred or used by existing VMs irrespective of file path location. If ISO files are not available for selection then you can specify the path manually.	N/A

Table 12-4 Other things to know *(continued)*

Issue	Description	Article link
Change in the preconfigured Virtual Machine Management Inventory task instance.	The preconfigured Virtual Machine Management inventory task instance is updated to let you edit and delete the task instance. By default, the task is configured to run at 6:30 P.M. daily on all discovered hypervisors. After the preconfigured VMM Inventory task instance is updated, the default schedule is changed based on the modified schedule.	N/A
Prerequisites for the **Shut Down** and **Restart** power control options support.	Before performing the **Shut Down** or **Restart** task, ensure that the following prerequisites are met: ■ Virtual machine is in **Power ON** state. ■ Operating system is running on the virtual machine. ■ VMware Tools for VMware or Integration Services for Hyper-V, is installed on the virtual machine. Currently, the **Shut Down** and **Restart** tasks are not available for all the guest operating system types.	N/A
Enable the Hyper-V server to work with remote WMI calls.	Hyper-V server communication uses the WMI protocol. The default firewall settings block WMI connections. You must enable Hyper-V server to work with WMI calls.	N/A
Additional information about the **Create Virtual Machine** wizard.	You need to select a Deployment Solution job only in the last step of the wizard that includes the partition task and the **Scripted Operating System Install** task.	N/A

Chapter 13

Workflow Solution

This chapter includes the following topics:

- What's new in Workflow Solution
- Known issues
- Fixed issues

What's new in Workflow Solution

In Workflow Solution 7.5 SP1, the following new features are introduced:

Table 13-1 List of new features in Workflow Solution 7.5 SP1

Feature	Description

Modification of Integration Component generators	The Integration Component generators are modified to use T4 text templates instead of NVelocity templates.
	To accommodate this change, the following NS6 generators are removed:
	■ Three NS6 pre-created generator projects as follows:
	  ■ Symantec.Components.Generated.Altiris.ASDK
	  ■ Symantec.Components.Generated.Altiris.ASDKTask
	  ■ Symantec.Components.Generated.Altiris.Resource
	■ Reports component generator for NS6 version
	■ Remedy generator
	■ Ensemble generator
	■ Profile service generator

Table 13-1 List of new features in Workflow Solution 7.5 SP1 *(continued)*

Feature	Description
Replacement of SyncFusion library	The SyncFusion libraries are replaced in Workflow Solution. Following are the affected areas: ■ Formula components in `LogicBase.Components.Calc.dll` The **Formula** component and the **Formula Equals Value Rule** component are now replaced with the custom component that implements the following most commonly-used operations: ■ Add ■ Subtract ■ Multiply ■ Divide ■ Average ■ RAND (Random Number) ■ STDEV (Standard Deviation) ■ IRR (Internal Rate of Return) ■ NPV (Net Present Value)

Table 13-1 List of new features in Workflow Solution 7.5 SP1 *(continued)*

Feature	Description
Replacement of SyncFusion library	■ Microsoft Office components Microsoft Office components that were previously found in `LogicBase.Components.Office.dll` are replaced with components built using the Microsoft Software Development Kit (SDK). As a result, only the new file formats `.docx` and `.xlsx` are supported. The `.doc` and `.xls` file formats are no longer supported. Following are the affected **Office** components: ■ Excel Configuration Based Editing (Model) component that includes the following components: ■ Excel Get Action ■ Excel Replace Action ■ Excel Run Macro Action ■ Excel Get Value ■ Excel Replace Value ■ Excel Write ■ Linked Word Merge ■ Word Merge ■ Convert Word To Text ■ Word Model ■ Append Document Action ■ Document Background Action ■ Document Properties Action ■ Insert Break Action ■ Insert Comment Action ■ Insert Footnote Endnote Action ■ Insert Hyperlink Action ■ Insert Image Action ■ Insert List Action ■ Insert Merge Field Action ■ Insert Table Action ■ Insert Text Action ■ Page Numbers Action ■ Replace Text Action ■ **Excel** generator ■ **Script** generator

Known issues

The following are the known issues for this release. If a workaround or other information about an issue is available, the issue has a corresponding article link.

Table 13-2 Known issues in this release

Issue	Description	Article link
JavaScript error is encountered in Internet Explorer 9 on expanding or collapsing groupings, resizing columns, or sorting columns.	When you log on to the Process Manager portal using Internet Explorer 9, click the **My Tasks Lists** tab, and expand, collapse, group, resize, or sort the columns, the JavaScript functionality is lost. The loss of functionality occurs shortly after the page refreshes. The following error message is displayed in Internet Explorer 9: `SCRIPT5007: Unable to get value of the property 'init' object is null or undefined ig_WebGrid_dom.js, line 4911 character 2.`	N/A
Cannot start Workflow Designer tool on computers on which User Account Control (UAC) is enabled.	The Windows Explorer does not have permissions to access the Workflow Designer executable file. Additionally, the following error message is displayed: `Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.` **Workaround**: Execute the Windows Explorer using **Run as Administrator** privilege. Then start the Workflow Designer tool using the Windows Explorer instance that has full administrative privileges.	N/A
Linked Word Merge component and Word Model component does not support .doc file format.	Microsoft Office components, which are found in `LogicBase.Components.Office.dll`, are now replaced with components built using the Microsoft Software Development Kit (SDK). As a result, only the new file formats `.docx` and `.xlsx` are supported. The `.doc` and `.xls` file formats are no longer supported.	N/A
Cannot execute the components which the Script Generator generates using multiple output paths.	Components, which the Script Generator generates using multiple output paths in string output only, are executed successfully. Components that are generated using multiple output path's variables other than string data type, display the following error message during execution: `The path <a variable or value of the project> is not contained in component <Component name>`	N/A

Table 13-2 Known issues in this release *(continued)*

Issue	Description	Article link
Script Generator fails to return multiple output paths using variables in data types other than string data type.	Script Generator wizard returns multiple output paths using variables in string data type only. On selecting multiple paths with variables in data types other than string, the Script Generator wizard displays the following error message during project compilation: `Cannot implicitly convert type 'any non- string data type' to 'string'`	N/A
Font size and text indentation do not work correctly in the HTML Editor component.	On changing the font size in the HTML editor, the cursor moves to the start of the field, and the changes are applied for newly-added content only. The changes are not applied to existing text. Additionally, on changing the text indentation of a line or text, the indentation of the entire content is changed. You cannot apply text indentation to specific text or line.	N/A
Error is encountered when the character font is set for the **Word Model** component.	Object reference error is encountered if character format is not specified while configuring the Office action components for **Word Model** component. If the character font is specified, then the **Word Model** component is executed without any errors.	N/A
Blank check box is displayed for Web Application project types.	Blank check box is displayed for Web Application project types on the **Workflow Enterprise Management Published Workflows page**.Therefore, you cannot filter published Web Application project types.	N/A

Fixed issues

The following are the issues from the previous releases that are fixed in this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 13-3 Fixed issues in this release

Issue	Description	Article link
The **Process View** page fails to load after you delegate one user's tasks to another user.	If you have delegated one user's tasks to another user using the **Manage Delegations** page of **Process Manager** portal, then the **Process View** page fails to load. This error occurs because the check to avoid loops fails to execute. Therefore, the delegation of tasks causes the Windows Process Activation Service (WAS) errors and the Application Pools to stop responding. The check to avoid loops now executes successfully, and the **Process View** page is displayed successfully.	N/A
Pass-through authentication is not available on non-Internet Explorer browsers, because of JavaScript errors.	Pass-through authentication now works for Process Manager login component on non-Internet Explorer browsers, such as Mozilla Firefox and Google Chrome. You are now not required to enter your login credentials manually, after you log on to the **Process Manager** portal with pass-through authentication using both Internet Explorer non-Internet Explorer browsers.	N/A
Localization errors displays odd characters in Web Parts after the browser language is set to French Canada, French France, or German.	No odd characters are now displayed in Web Parts if the browser language is set to French Canada, French France or German.	N/A
SharePoint Generator components do not work with SharePoint Server 2010 and SharePoint Server 2013, because of authentication errors.	The generated SharePoint components now authenticate correctly with SharePoint Server 2010 and SharePoint Server 2013.	N/A
Document Category View page of **Process Manager** portal shows incorrect number of attachments, if more than 10 documents are attached and the attachments are added outside the **Category View** page.	The **Document Category View** page of **Process Manager** portal now shows exact number of attached documents.	N/A

Table 13-3 Fixed issues in this release *(continued)*

Issue	Description	Article link
Execute Process and Wait (Run) component does not retrieve the exit code from external applications.	After you execute a project, the Execute Process and Wait (Run) component now retrieves exit code of the external applications.	N/A
License Status Manager tool displays extraneous characters when launched on the operating systems whose language is set to German.	No extraneous characters are found if the License Status Manager tool is now launched on the operating systems whose language is set to German.	N/A
Object reference error is encountered when a report is exported to Microsoft Excel.	Using the **Process Manager** portal, you can now export reports to Microsoft Excel successfully.	N/A
Cannot publish Windows Service and Task Tray application projects to an installer.	You can now publish the Windows Service projects and Task Tray application projects to an installer using ServiceDesk and Workflow Solution.	N/A
The Service Catalog Web Part displays all the Service Catalog items to all users.	During adding a Service Catalog Web Part, the Service Catalog items are now displayed based on the permissions that are assigned to the user account. No Service Catalog items are displayed if the user account does not have the required permissions.	N/A
New users are not synced in **Process Manager** portal if field mapping is used in Active Directory sync profile.	Both the existing users and the new users are now synced in **Process Manager** portal if the field mapping is used in Active Directory sync profile.	N/A
Add Report Category icon is displayed to all users who can access the reports in **Reports** tab.	The **Add Report Category** icon is now displayed and is available for use based on the permissions that are assigned to the user account. The icon is not displayed and the reports cannot be accessed if the user account does not have the required permissions.	N/A
The **Show More** link on knowledge base tab of **Process Manager** portal does not show complete article contents in a separate dialog box, for the articles that had an apostrophe (') in title.	The **Show More** link on **knowledge base** tab of **Process Manager** portal now shows complete article contents in a separate dialog box.	N/A

Table 13-3 Fixed issues in this release *(continued)*

Issue	Description	Article link
The Post Office Protocol 3 (POP3) Get component does not support STARTTLS.	The TLS1 option of the SSL type is now removed, because the POP3 Get component does not support STARTLS.	N/A
Cannot specify a configurable timeout value from the SQL **Connection String Editor** page.	You can now specify a configurable timeout value in the **Sql Connection String** field on the SQL **Connection String Editor** page.	N/A
Listbox on a form does not save the selection, if you navigated to some other page and then returned on the form page.	The List Box component on the form now saves your selected options, even if you navigate to some other page and then return to the form page.	N/A
The **Show More** link on **knowledge base** tab of **Process Manager** portal is broken, after the knowledge base article text was truncated to fit into the **All Articles** list.	The **Show More** link now directs you to the article, even after the knowledge base article text is truncated to fit into the **All Articles** list.	N/A
When the Web Part is closed, the Web Part is permanently closed or hidden to all users.	The **Allow Close** check box is now removed from the **Process History Settings** page of a Web Part on the **Process Manager** portal. The Web Part is now displayed to all users.	N/A
Changes in the **Process View** page are displayed only to the new users, who have never logged on to the ServiceDesk portal.	If the administrator user makes any changes on the **Process View** page, then the changes are now displayed to both the existing users and the new users.	N/A
If a **Process View** page that has large history data is printed in Internet Explorer 8 or 9, the Process History type Web Parts are broken, and the data is not printed.	The entire history data of the **Process View** page is now printed successfully.	N/A
The Active Directory authentication fails during accessing the Form Workflow projects because of URL mismatch.	The Active Directory authentication now executes successfully, and lets you access the **Process Manager** portal as well as the Form Workflow projects.	N/A

Table 13-3 Fixed issues in this release *(continued)*

Issue	Description	Article link
During printing a **Process View** page, the green tick mark icon and red cross icon are not displayed.	During printing a **Process View** page, the green tick mark icon and red cross icon are now displayed as per the **Admin**, **Edit**, and **View** permission settings.	N/A
During processing an incident, the **Process Permissions** Web Part is displayed as minimized on startup, regardless of the Web Part setting.	The **Process Permissions** Web Part is now displayed as minimized if the **Minimized On Startup** check box is selected in Web Part settings. If the **Minimized On Startup** check box is not selected, then the Web Part is displayed as maximized or minimized as per the initial configured setting.	N/A